

2011

A new emergency control method and a preventive mechanism against cascaded events to avoid large-scale blackouts

Jie Yan

Iowa State University

Follow this and additional works at: <https://lib.dr.iastate.edu/etd>

 Part of the [Electrical and Computer Engineering Commons](#)

Recommended Citation

Yan, Jie, "A new emergency control method and a preventive mechanism against cascaded events to avoid large-scale blackouts" (2011). *Graduate Theses and Dissertations*. 10334.
<https://lib.dr.iastate.edu/etd/10334>

This Dissertation is brought to you for free and open access by the Iowa State University Capstones, Theses and Dissertations at Iowa State University Digital Repository. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.

A new emergency control method and a preventive mechanism against cascaded events to avoid large-scale blackouts

by

Jie Yan

A dissertation submitted to the graduate faculty
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Electrical Engineering

Program of Study Committee:
Chen-Ching Liu, Major Professor
Lizhi Wang
Manimaran Govindarasu
Umesh Vaidya
Venkataramana Ajjarapu

Iowa State University
Ames, Iowa
2011

Copyright @ Jie Yan, 2011. All rights reserved.

DEDICATION

This dissertation is dedicated to my love Ningning Zhang, for being the light of my life.

TABLE OF CONTENTS

LIST OF FIGURES	v
LIST OF TABLES	vi
ABSTRACT	vii
CHAPTER 1. INTRODUCTION.....	1
1.1 Cascaded Events.....	1
1.2 Countermeasures	2
1.3 Research Scope.....	4
CHAPTER 2. PMU-BASED MONITORING OF ROTOR ANGLE STABILITY.....	6
2.1 State-of-the-art.....	6
2.2 Problem Formulation.....	7
2.3 Methodology: Lyapunov Exponents	9
2.4 On-line Monitoring Scheme	13
2.5 Computation Method.....	15
2.5.1 Spectrum Analysis.....	16
2.5.2 Implicit Integration Method With Trapezoidal Rule	16
2.5.3 Gram-Schmidt Reorthonormalization (GSR).....	17
2.6 Simulation Results.....	19
2.6.1 3-machine System	19
2.6.2 200-bus System	21
2.6.3 Sensitivity Analysis.....	25
2.6.4 Computational Burden.....	27
2.7 Discussion	27
CHAPTER 3. RISK ASSESSMENT FOR CYBER SECURITY	28
3.1 State-of-the-art.....	28
3.2 Risk Assessment Framework	29
3.2.1 Duality Element Relative Fuzzy Evaluation Method	30
3.2.2 Attack Graph	31
3.2.3 Intrusion Response System.....	35
3.3 Proposed Algorithm.....	36
3.3.1 Dynamical Model	36
3.3.2 Methodology: Conditional Lyapunov Exponents.....	38

3.3.3	Application of MCLE.....	39
3.3.4	Computation Method.....	40
3.3.5	Control Actions	41
3.4	Case Study	41
3.4.1	Wind Farm SCADA Systems	42
3.4.2	Security Vulnerabilities	43
3.4.3	DERFEM and Attack Graph	50
3.4.4	Simulation Results.....	54
3.5	Discussion	59
CHAPTER 4. CONCLUSIONS		60
PUBLICATIONS		62
BIBLIOGRAPHY		63
ACKNOWLEDGEMENTS		71

LIST OF FIGURES

Fig. 1.1.	The common process of cascaded events.....	1
Fig. 1.2.	The countermeasures against cascaded events.....	3
Fig. 2.1.	Nearby trajectories in the state space.....	10
Fig. 2.2.	The diminishing separation.....	12
Fig. 2.3.	The colliding trajectories.....	12
Fig. 2.4.	The concept for monitoring of rotor angle stability.....	14
Fig. 2.5.	The standard method with GSR.....	17
Fig. 2.6.	A 3-machine system.....	19
Fig. 2.7.	The time-domain simulation result for the 3rd contingency.....	21
Fig. 2.8.	A 200-bus system.....	22
Fig. 2.9.	The time-domain simulation results and the approximation results for comparison ...	23
Fig. 3.1.	The proposed risk assessment framework.....	30
Fig. 3.2.	Concept of IRS.....	35
Fig. 3.3.	Nearby trajectories in the state space.....	38
Fig. 3.4.	The generic network configuration of wind farm SCADA systems.....	43
Fig. 3.5.	A chemical combinatorial attack.....	45
Fig. 3.6.	An example of tapping.....	47
Fig. 3.7.	The actual tap hardware.....	48
Fig. 3.8.	The constructed attack graph.....	51
Fig. 3.9.	IEEE 10 Generator 39 Bus System.....	54
Fig. 3.10.	The simulation results.....	59

LIST OF TABLES

Table 2.1. The simulation results of the 3-machine system	20
Table 2.2. The simulation results of the 200-bus system	24
Table 2.3. The sensitivity analysis results	25
Table 3.1. The comparison results of the vulnerabilities.....	31
Table 3.2. The results of DERFEM.....	51
Table 3.3. The intrusion scenarios and the probabilities	54
Table 3.4. MCLE of bus G3	56

ABSTRACT

Cascaded events may cause a major blackout which will lead to a massive economic loss and even fatalities. Significant research efforts have been made to address the issue systematically: preventive mechanisms are designed to mitigate the impact of initiating events on power systems; emergency control methods are proposed to prevent power systems from entering an unstable state; restorative control methods are developed to stop the propagation of power system instability and to prevent widespread blackouts.

This work contributes to the development of new emergency control methods and preventive mechanisms.

First, a new emergency control scheme is proposed for preventing power systems from a loss of synchronism. Traditional out-of-step relays may fail to predict losses of synchronism as the dynamics of power systems become more and more complex. In recent years, the installation of the Phasor Measurement Units (PMUs) on power grids has increased significantly and, therefore, a large amount of real-time data is available for on-line monitoring of power system dynamics. This research proposes a PMU-based application for on-line monitoring of rotor angle stability. The Lyapunov Exponents are used to predict a loss of synchronism within large power systems. The relationship between rotor angle stability and the Maximal Lyapunov Exponent (MLE) is established. A computational algorithm is developed for the calculation of MLE in an operational environment. The effectiveness of the monitoring scheme is illustrated with a 3-machine system and a 200-bus system model.

Then, a preventive mechanism against cyber attacks is developed. Cyber threats are serious concerns for power systems. For example, hackers may attack power control

systems via the interconnected enterprise networks. This research proposes a risk assessment framework to enhance the resilience of power systems against cyber attacks. The Duality Element Relative Fuzzy Evaluation Method (DERFEM) is employed to evaluate identified security vulnerabilities within cyber systems of power systems quantitatively; The Attack Graph is used to identify possible intrusion scenarios that exploit multiple vulnerabilities; an Intrusion Response system (IRS) is developed to monitor the impact of intrusion scenarios on power system dynamics in real time. IRS calculates the Conditional Lyapunov Exponents (CLEs) on line based on PMU data. Power system stability is predicted through values of CLEs. Control actions based on CLEs will be suggested if power system instability is likely to happen. A generic wind farm control system is used for case study. The effectiveness of IRS is illustrated with the IEEE 39 bus system model.

CHAPTER 1. INTRODUCTION

1.1 Cascaded Events

Cascaded events are identified as causes of recent large-scale blackouts around the world, such as the 1996 blackout in U.S. [1], the 2003 blackout in North America [2], the 2003 blackout in Italy [3], and the 2006 blackout in Europe [4]. The resultant blackouts brought about massive economic losses, widespread panics, and failures of essential services. For example, the 2003 blackout was estimated to cost about \$6 billion [5], and it contributed to 11 reported fatalities.

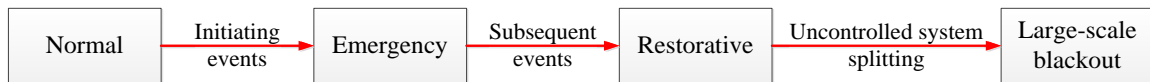


Fig. 1.1. The common process of cascaded events

Cascaded events in major blackouts follow a common process [6], as shown in Fig. 1.1. Typically, cascaded events are initiated by a single or multiple events, such as the 500-kV line outage (U.S. 1996), the generator tripping and 345-kV line outage (U.S. and Canada 2003), the line outage (Italy 2003) and the coupling operation of busbars at a substation (Europe 2006). The initiating events result in violations of operating constraints of power systems, and then drive systems from a normal state into an emergency state. The violations of operating constraints, if not corrected in time, can trigger successive line tripping and/or generator tripping events. These subsequent events cause a significant imbalance between power supply and load, and move power systems into a restorative state. Frequency instability, voltage instability and rotor angle instability can take place during system restoration, leading to an uncontrolled system

splitting. The excessive imbalance between load and generation after the uncontrolled system splitting eventually leads to a large-scale blackout.

Initiating events in this context include: natural calamities, power system component failures, protection and control system malfunctions, information and communication system failures, system instability due to disturbances, human errors, inadequate security assessment procedures, gaming in the electricity market, sabotages, intrusions by external agents, and missing or uncertain information in decision making [7].

Common emergency states include overloading and over-excitation. These vulnerable operating conditions can trigger corresponding relay actions such as line tripping due to overloading, and generator tripping due to over-excitation. The relay actions may further weaken power systems, and result in subsequent events. For example, tripping of an overloaded line leads to a power flow rerouting, and then the remaining lines have to deliver more power, which may cause overloading in the transmission network, and hence successive line tripping events.

Restorative states include loss of synchronism, and abnormal system voltage and frequency. In a restorative state, load and generator tripping events spread promptly, which may initiate an uncontrolled system splitting.

1.2 Countermeasures

Much effort has been made to improve the reliability of power systems against cascaded events. Current research is focused on three areas: preventive mechanisms, emergency controls, and restorative controls, as shown in Fig. 1.2.

Preventive mechanisms are to mitigate the impact of initiating events on power systems. If one wants to develop the preventive mechanism against a given class of initiating events for power systems, the probability of occurrence of every initiating event should be evaluated, the resultant impact should be assessed quantitatively, and then mitigation mechanisms can be proposed based on a cost-effectiveness analysis. In [8], the impact of a massive measurement loss on power system state estimation is evaluated. The results suggest that the inclusion of injection pseudo measurement provides a stable state estimation with acceptable errors. In [9], lightning-related failure rate of power system equipment is evaluated by a formalized method. Insulation coordination of power system equipment is suggested consequently. In [10], animal-caused faults in power distribution systems are discussed and analyzed. An effective method to prevent such faults is presented.

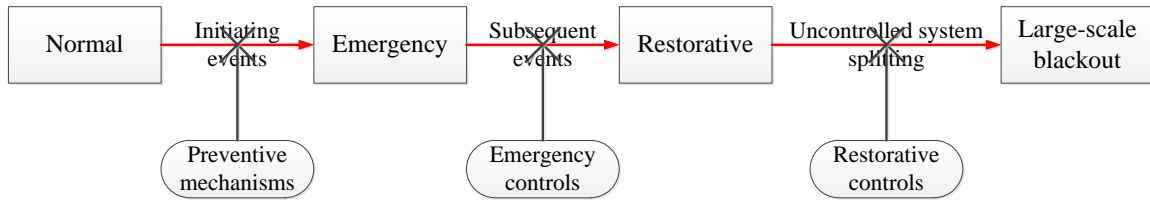


Fig. 1.2. The countermeasures against cascaded events

Emergency controls are employed to prevent power systems from entering restorative states. Emergency controls typically involve monitoring of power systems in real time (especially power system dynamics), coordinated relay actions, and corrective control actions. In [11], voltage stability of a power system is monitored in real time by an artificial neural network based method. Voltage stability margin is calculated in real time based on wide-area measurements. Voltage stability control actions are initiated according to the estimated voltage stability margin. In [12], power system stability is

evaluated after a disturbance, so as to identify whether or not power systems will return to a stable operating point. A system protection scheme is proposed to bring an unstable operating point back inside a stable region in order to avoid cascaded voltage collapses. In [13], transient stability is assessed in real time by monitoring generator angles and angular speeds. In [14], frequency stability after a contingency is predicted by a novel predictive method. Stabilizing load shedding is determined in a coordinated way.

Restorative controls are used to stop the propagation of power system instability, in order to prevent a widespread blackout. Typical restorative control actions include generator output adjustment, controlled generator tripping, load shedding, and system islanding. Reference [15] proposes a self-healing system reconfiguration method that intentionally splits a power network under a contingency into self-sufficient islands to avoid catastrophic failures.

1.3 Research Scope

This work contributes to the development of new emergency control methods and preventive mechanisms.

First, a new emergency control scheme is proposed for preventing power systems from entering one of the severe operating conditions: loss of synchronism. Rotor angle stability of power systems has been a challenging task as the dynamics of power systems become more and more complex. Traditional out-of-step relays predict a loss of synchronism in the first power swing after clearance of disturbances. Nevertheless, severe disturbances such as double faults along both circuits of double-circuit lines might cause a loss of synchronism in swings after the first swing. As a result, rotor angle stability cannot be easily predicted. However, the advent of the Phasor Measurement

Units (PMUs), together with advances in computational and communications facilities, provides an opportunity to perform on-line monitoring of power system dynamics. This research proposes a PMU-based application for on-line monitoring of rotor angle stability.

Then, a preventive mechanism against cyber attacks is developed. Power systems are vulnerable to cyber attacks. Modern IT technologies are heavily used in today's Supervisory Control And Data Acquisition (SCADA) systems of industrial control systems including power systems. While IT technologies bring a lot of benefits, many security risks are introduced as well. For example, the connectivity of SCADA systems and enterprise networks improves business visibility and efficiency, but it makes SCADA systems more vulnerable to cyber attacks. According to the 2003-2006 data from Eric Byres, BCIT, 49% cyber attacks at industrial control systems are launched via the connected enterprise networks. One highly publicized example is Stuxnet, which attacked an industrial control system by infecting those organization networks that interact with the target [16]. This work proposes a systematic method for risk assessment to address issues arising from cyber threats.

CHAPTER 2. PMU-BASED MONITORING OF ROTOR ANGLE STABILITY

2.1 State-of-the-art

The first version of a PMU-based out-of-step relay is applied to the Florida-Georgia system in [17]-[20]. The system is modeled as two interconnected equivalent generators. Then two PMU sets are used to monitor the angular difference between these two equivalent generators. Based on the monitored angular difference, the Equal Area Criterion (EAC) is utilized to distinguish between an unstable power swing and a stable one. In [21], the Energy Function Analysis is used to monitor rotor angle stability. Reference [22] reports an out-of-step prediction logic based on an autoregressive model (AR model). A method for monitoring an inter-area oscillation mode by spectrum analysis is presented in [23]. The results of [22-23] represent forecasting procedures based on time-series analysis of PMU data during power swings. In [24], synchronized phasor measurements are used as the input for the computation of the differential/algebraic equation (DAE) model of post-fault power systems. Then, the numerical results are used for prediction. A fuzzy neural network based on PMUs is applied to power swing stability prediction [25]. In [26], a self-adaptive Decision Tree (DT) approach for on-line dynamic security assessment is presented. Offline contingency analysis data such as PMU data is used to identify critical attributes of DT nodes and to train DT. In [27], large-size DTs extracting selected decision features from PMU measurements are used for rapid stability assessment. The technique involves an off-line study. In [28], neural networks are used to estimate rotor angles for on-line monitoring of transient stability based on PMU measurements.

In this work, an analytical method is proposed for monitoring wide-area rotor angle stability in an operational environment using PMU data. Power systems are modeled as a multi-bus system. The Maximal Lyapunov Exponent (MLE) is employed to determine whether or not a power swing indicates a loss of synchronism. The method provides a high level of accuracy with a low computational burden.

The application of the Lyapunov Exponents is proposed in [29]. Their work indicates that the Lyapunov Exponents can be used to predict out-of-step conditions. The result is supported by simulation results with a small power system. The proposed method in this research extends the work of [29] by articulating the mathematical relationship between the Lyapunov Exponents and loss of synchronism conditions. Furthermore, the connection between MLE and rotor angle stability of power systems is established. An efficient computational algorithm is proposed for the calculation of MLE based on a finite time window of PMU data. The effectiveness of the proposed method is validated by simulation results with a 3-bus system and a 200-bus system.

2.2 Problem Formulation

Rotor angle stability is concerned with the ability of power systems to maintain synchronism when subjected to a small or large disturbance. Power system faults and line switching result in a sudden change on generator outputs. However, mechanical power inputs to generators do not change instantaneously. These major disturbances can cause severe oscillations in machine rotor angles and severe swings in power flows. A loss of synchronism can occur between one generator and the rest of the system, or between groups of generators, leading to instability conditions. This research is concerned with the prediction of rotor angle instability following disturbances on power systems. The goal of

this research is to develop a practical application of PMU data together with mathematical and computational foundations.

A power system with n buses and $m+1$ generators represented by a dynamical model is considered. The generators are modeled by classical equations, while the loads are represented by ZIP models. Assume that mechanical power inputs to the generators are constant during a contingency period. The system model can be represented by:

$$\begin{cases} \frac{d\delta_i^D}{dt} = \omega_i^D \\ \frac{d\omega_i^D}{dt} = h_i(\boldsymbol{\delta}^D, \boldsymbol{\omega}^D) \end{cases} \quad (2.1)$$

where $i=1,2,\dots,m$, $\boldsymbol{\delta}^D = (\delta_1^D, \dots, \delta_m^D)^T$, $\boldsymbol{\omega}^D = (\omega_1^D, \dots, \omega_m^D)^T$, δ_i^D is the relative rotor angle of generator i , ω_i^D is the relative angular speed of generator i , and h_i is a nonlinear function of $\boldsymbol{\delta}$ and $\boldsymbol{\omega}$.

Prior to a disturbance, the power system is represented by a $2m$ -dimensional continuous-time dynamical system denoted by:

$$\frac{dx}{dt} = \mathbf{f}_S(\mathbf{x}) \quad (2.2)$$

where $\mathbf{x} = (\delta_1^D, \dots, \delta_m^D, \omega_1^D, \dots, \omega_m^D)^T$. \mathbf{f}_S represents the vector of nonlinear functions of the dynamical system that represents the power system in a pre-disturbance steady state.

After a disturbance, parameters of the model are updated as necessary in order to establish a nonlinear dynamical system to represent the power system during the contingency period.

$$\frac{dx}{dt} = \mathbf{f}_{Tr}(\mathbf{x}) \quad (2.3)$$

where \mathbf{f}_{Tr} represents the vector of nonlinear functions of the dynamical system that represents the power system during the contingency period. The nonlinear system trajectory $\mathbf{x}_{Tr}(t)$ in the state space is the power swing curve following the disturbance.

The nonlinear system is said to be stable if and only if $\mathbf{x}_{Tr}(t)$ approaches an asymptotically stable equilibrium point, which means $\mathbf{x}_{Tr}(t)$ arrives at, and stays within the attractor of an asymptotically stable equilibrium point. The generators maintain synchronism if the nonlinear system is asymptotically stable. The proposed method in this work is used to assess nonlinear system stability, and hence rotor angle stability. Assessing local stability by linearizing around an equilibrium point is a special case of the method.

Note that $\mathbf{x}_{Tr}(t)$ represents a post-fault system trajectory. The brief fault-on period from the occurrence of a fault to relay tripping, breaker opening (and possible breaker reclosure) is not explicitly modeled. The fault-on period will affect system states and hence initial conditions of the post-fault period. The proposed method is intended for monitoring of the electromechanical dynamics of power systems from the initial condition of the post-fault period.

2.3 Methodology: Lyapunov Exponents

MLE of $\mathbf{x}_{Tr}(t)$ is calculated to monitor rotor angle stability after a disturbance. If MLE is negative, it is concluded that $\mathbf{x}_{Tr}(t)$ will approach an asymptotically stable equilibrium point, and hence the power swing is (asymptotically) stable. For the proposed method, if MLE is higher than or equal to zero, it is judged that $\mathbf{x}_{Tr}(t)$ will not approach any asymptotically stable equilibrium point, and the power swing is considered “unstable”, which, strictly speaking, means “not asymptotically stable” in this context of this work.

The Lyapunov Exponents and their relationship with system stability are discussed in the following. In ergodic theory of dynamical systems, the Lyapunov

Exponents are used to characterize the exponential divergence or convergence of nearby trajectories as shown in Fig. 2.1. For an N -dimensional continuous-time dynamical system $\frac{dx}{dt} = \mathbf{f}(\mathbf{x})$, let $\mathbf{x}(t) = \boldsymbol{\varphi}(t, \mathbf{v})$ be the solution at time t starting from the initial condition $\mathbf{v} = \mathbf{x}_0$. The Lyapunov Exponents λ_i for $i=1, \dots, N$ are defined as eigenvalues of the following limiting.

$$\begin{aligned} \Lambda(\mathbf{v}) &= \lim_{t \rightarrow \infty} [\mathbf{K}^T(t, \mathbf{v}) \mathbf{K}(t, \mathbf{v})]^{1/2t} \\ \lambda_i(\mathbf{v}) &= \ln[\bar{\lambda}_i(\mathbf{v})] \end{aligned} \quad (2.4)$$

where $\mathbf{K}(t, \mathbf{v}) = \text{matrix}[\partial \varphi_i(t, \mathbf{v}) / \partial v_j]$, $\mathbf{K}^T(t, \mathbf{v})$ is the transpose of $\mathbf{K}(t, \mathbf{v})$, and $\bar{\lambda}_i(\mathbf{v})$ is the i th eigenvalue of $\Lambda(\mathbf{v})$.

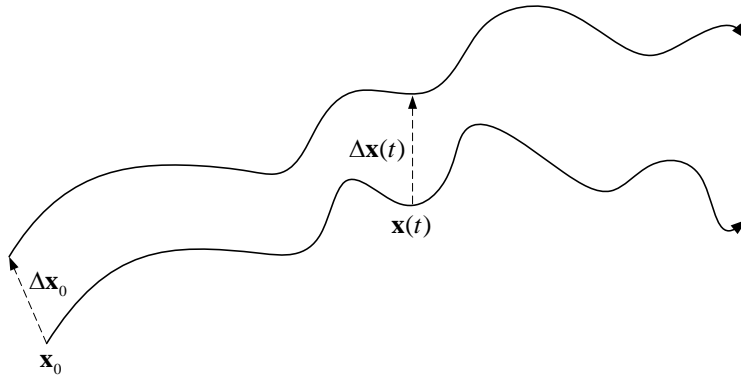


Fig. 2.1. Nearby trajectories in the state space

The limit in (2.4) is known to exist by Oseledec multiplicative ergodic theorem [30]. For the purpose of the proposed application, the following index is defined.

$$\lambda = \lim_{t \rightarrow \infty} [t^{-1} \ln \|\mathbf{K}(t, \mathbf{v}) \Delta \mathbf{v}\|] \quad (2.5)$$

where $\Delta \mathbf{v} = \Delta \mathbf{x}_0$ is a randomly chosen vector in small scale, as shown in Fig. 2.1. λ in (2.5) is MLE. A negative (positive) value of λ implies the exponential convergence (divergence, respectively) of nearby system trajectories. This is true due to the approximation of

$$\|\Delta \mathbf{x}(t)\| \approx e^{\lambda t} \|\Delta \mathbf{x}_0\| \quad (2.6)$$

In this research, the relationship between MLE and asymptotic behavior of a dynamical system is established based on the results of [31].

MLE Stability Criterion: Consider a continuous-time dynamical system and assume that all the Lyapunov exponents are nonzero. Then the steady state behavior of the system consists of a fixed point. Furthermore, if MLE is negative, then the steady state behavior is an attracting fixed point.

Outline of Proof: Consider a N -dimensional continuous-time dynamical system $\frac{d\mathbf{x}}{dt} = \mathbf{f}(\mathbf{x})$, \mathbf{f} is differentiable, and $\mathbf{x} \in \mathbf{X} \subset R^N$, where \mathbf{X} is a compact set. If the initial point $\mathbf{x}(0)$ is given, then there is a corresponding trajectory $\mathbf{x}(t)$ in the N -dimensional phase space. There also exist N Lyapunov Exponents for $\mathbf{x}(t)$ according to the definition of the Lyapunov Exponents.

Definition 2.1 [32]. The equilibrium point \mathbf{x}_{eq} is

- Stable if, for each $\varepsilon > 0$, there is $\theta = \theta(\varepsilon) > 0$ such that

$$\|\mathbf{x}(0) - \mathbf{x}_{eq}\| < \theta \Rightarrow \|\mathbf{x}(t) - \mathbf{x}_{eq}\| < \varepsilon, \forall t \geq 0$$

- asymptotically stable if it is stable and θ can be chosen, such that

$$\|\mathbf{x}(0) - \mathbf{x}_{eq}\| < \theta \Rightarrow \lim_{t \rightarrow \infty} \|\mathbf{x}(t) - \mathbf{x}_{eq}\| = 0$$

Now define $\frac{d\mathbf{y}}{dt} = \mathbf{f}(\mathbf{y})$ with an arbitrary initial point $\mathbf{y}(0)$. Then there is another trajectory $\mathbf{y}(t)$ in the state space. According to the definition of the Lyapunov Exponents, if MLE of $\mathbf{x}(t)$, $\lambda < 0$, $\exists \varepsilon_1 > 0$, such that

$$\|\mathbf{y}(0) - \mathbf{x}(0)\| < \varepsilon_1 \Rightarrow \lim_{t \rightarrow \infty} \|\mathbf{y}(t) - \mathbf{x}(t)\| = 0$$

Hence, the separation between the trajectories $\mathbf{x}(t)$ and $\mathbf{y}(t)$ will diminish to 0 as time

goes on, if $\lambda < 0$ and the initial points $\mathbf{x}(0)$ and $\mathbf{y}(0)$ are close enough, as Fig. 2.2 shows.

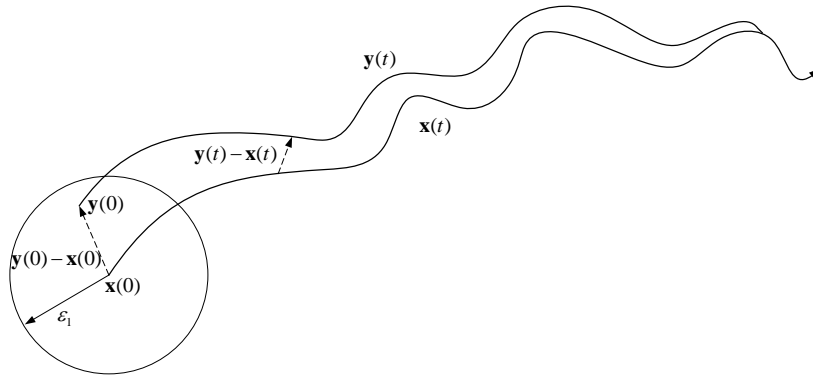


Fig. 2.2. The diminishing separation

If $\lambda < 0$, as mentioned before, $\exists \varepsilon_1 > 0$, such that

$$\|\mathbf{y}(0) - \mathbf{x}(0)\| < \varepsilon_1 \Rightarrow \lim_{t \rightarrow \infty} \|\mathbf{y}(t) - \mathbf{x}(t)\| = 0$$

Then $\exists \Delta T > 0$, such that $\|\mathbf{x}(\Delta T) - \mathbf{x}(0)\| < \varepsilon_1$. Let $\mathbf{y}(0) = \mathbf{x}(\Delta T)$, then $\mathbf{y}(t) = \mathbf{x}(t + \Delta T)$, since the dynamical system is autonomous, as Fig 2.3 shows.

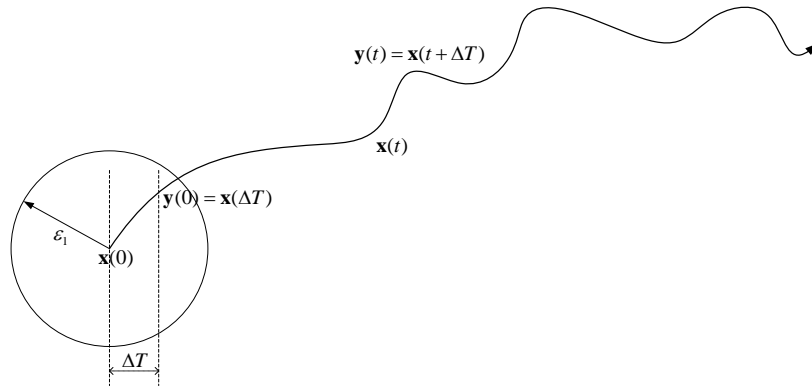


Fig. 2.3. The colliding trajectories

Hence

$$\lim_{t \rightarrow \infty} \|\mathbf{y}(t) - \mathbf{x}(t)\| = \lim_{t \rightarrow \infty} \|\mathbf{x}(t + \Delta T) - \mathbf{x}(t)\| = 0$$

Moreover

$$\lim_{t \rightarrow \infty} \|\mathbf{x}(t + \Delta T) - \mathbf{x}(t)\| \approx \lim_{t \rightarrow \infty} \|\mathbf{f}[\mathbf{x}(t)]\Delta T\|$$

Since $\Delta T > 0$,

$$\lim_{t \rightarrow \infty} \|\mathbf{f}[\mathbf{x}(t)]\| \approx 0$$

Therefore, $\mathbf{x}(t)$ will approach an equilibrium point, say \mathbf{x}_{eq} .

\mathbf{x}_{eq} can be viewed as a special trajectory: it starts at \mathbf{x}_{eq} , stays at \mathbf{x}_{eq} . The special trajectory of \mathbf{x}_{eq} has the same MLE as $\mathbf{x}(t)$ does. Then $\exists \varepsilon_2 > 0$, such that

$$\|\mathbf{y}(0) - \mathbf{x}_{eq}\| < \varepsilon_2 \Rightarrow \lim_{t \rightarrow \infty} \|\mathbf{y}(t) - \mathbf{x}_{eq}\| = 0$$

Hence, by Definition 2.1, \mathbf{x}_{eq} is asymptotically stable.

MLE stability criterion provides a sufficient condition for system stability when MLE is negative. If λ is positive or zero, nearby system trajectories will not converge according to (2.6). Suppose that the system trajectory $\mathbf{x}(t)$ has arrived at an equilibrium point \mathbf{x}_{eq} , and $\lambda \geq 0$. Assume that a small disturbance is applied, state variables move to another point near \mathbf{x}_{eq} . A new system trajectory will start at that point around \mathbf{x}_{eq} . Since $\lambda \geq 0$, the new trajectory will not get back to \mathbf{x}_{eq} . System instability is likely to occur. The probability cannot be measured accurately due to the chaotic nature of nonlinear systems. However, study shows that system instability occurs within practical systems when λ is positive or zero.

2.4 On-line Monitoring Scheme

The concept for on-line monitoring of rotor angle stability is illustrated in Fig. 2.4. It is intended to be an application in the control center of a power system. The proposed algorithm obtains updated power network configurations from the State

Estimator (SE), say, every 5 minutes.

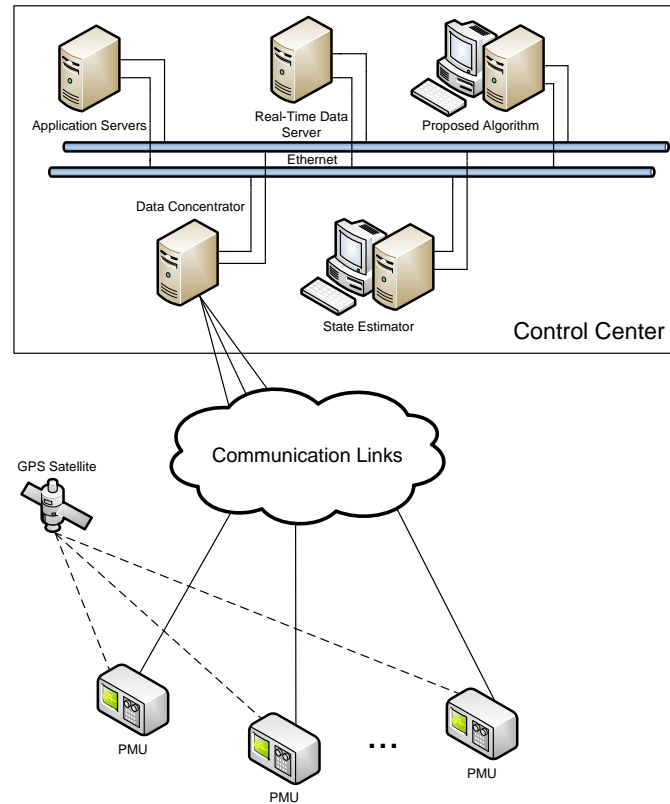


Fig. 2.4. The concept for monitoring of rotor angle stability

As discussed in Section 2.2, following a disturbance such as a fault and the corresponding relay and breaker responses, the sudden change of power network configurations is reported through SCADA systems in real time. There is a time delay before SCADA data arrives at the control center. Typically, the control center will receive SCADA data about the configuration change in a matter of seconds. For example, in California ISO, the transmission delay is less than 4 seconds. An updated post-fault dynamic model $\dot{\mathbf{x}} = \mathbf{f}_{Tr}(\mathbf{x})$ is then obtained by modifying related parameters according to SCADA data. After that, the proposed algorithm extracts synchronized phasor measurements from the PMU data concentrator, which obtains real time PMU data from substations equipped with PMUs. Hence, a number of the variables of $\mathbf{x}_{Tr}(t)$ are

observed from PMU data. Based on the updated dynamical system and PMU measurements after the disturbance, MLE index of $\mathbf{x}_{Tr}(t)$ is calculated by the algorithm which will be discussed in detail next. If MLE has a negative value, the prediction is that the power swing is stable; otherwise, it is unstable. Appropriate control actions will be needed.

If another disturbance occurs during the computation of MLE, and it changes the system configurations, the power system will be represented by another updated dynamical system consequently, and system stability will be re-assessed. MLE will be re-calculated based on the most current dynamical system model and PMU measurements after the event, in order to determine system stability.

2.5 Computation Method

A computationally efficient algorithm to calculate MLE is proposed. The calculation of MLE is based on (2.5). In practice, there are three difficulties:

- 1) One can only calculate $\lambda_{t=T}$, MLE over a finite time interval T , instead of λ over an infinite time interval as shown in (2.5). The length of time interval, T should be preselected properly so that $\lambda_{t=T}$ is able to predict short-term system stability and instability.
- 2) Complete observability of the trajectory $\mathbf{x}_{Tr}(t)$ is required in (2.5) to calculate its MLE, which means that rotor angles and angular speeds of all the generators in a power system are to be observed by PMU data. However, at present, there are only a limited number of PMUs in power systems.
- 3) A fast way to calculate MLE is required for on-line monitoring, since rotor

angle stability after a disturbance must be determined quickly to allow for effective control actions.

The above issues are addressed in the following.

2.5.1 Spectrum Analysis

Spectrum analysis is used to compute an appropriate time interval length T . In practice, power swings exhibit strong periodic behaviors, and the frequency lies within a narrow frequency band under a given system scenario. One can simulate all the credible disturbances on a power system in an off-line study, and obtain power swing curves following the disturbances. Spectrum analysis is then applied to the power swing curves to identify a frequency band. In this work, the R language is employed to conduct the spectrum analysis. Based on results of the spectrum analysis, T is set as the inverse ratio to the lower limit of the frequency band, so that it covers at least one cycle of the power swings. $\lambda_{t=T}$ has the capability to predict whether rotor angle instability will occur in swings after the first power swing.

2.5.2 Implicit Integration Method With Trapezoidal Rule

The Implicit Integration Method With Trapezoidal Rule is used to approximate the unobservable part of the state variables in $\mathbf{x}_{Tr}(t)$. The idea is to estimate the unobservable state variables at instant $j+1$ based on the estimated values of the unobservable state variables at instant j and the observed values of the observable state variables at instant j and $j+1$. For example, assume that the state variables x_1, x_2, \dots, x_k are monitored by PMUs, while the remaining variables are not. The state variables of $\mathbf{x}_{Tr}(0)$ are either observed or estimated. The unobservable state variables of $\mathbf{x}_{Tr}(\Delta t)$ are estimated by integration results of the dynamical system $\frac{dx}{dt} = \mathbf{f}_{Tr}(\mathbf{x})$, shown as follows:

$$\begin{aligned}
\mathbf{x}_{Tr}(\Delta t) &= \mathbf{x}_{Tr}(0) + \{\mathbf{f}_{Tr}[\mathbf{x}_{Tr}(\Delta t)] + \mathbf{f}_{Tr}[\mathbf{x}_{Tr}(0)]\} \cdot \Delta t/2 \\
x_1(\Delta t) &= x'_1(\Delta t) \\
&\vdots \\
x_k(\Delta t) &= x'_k(\Delta t)
\end{aligned} \tag{2.7}$$

where Δt is a predefined time step, and $x'_k(\Delta t)$ is the observed value of $x_k(\Delta t)$ at instant Δt by PMU data. The Newton-Raphson method is then applied to calculate an estimation of $\mathbf{x}_{Tr}(\Delta t)$. Note that for the next time increments, $\mathbf{x}_{Tr}(2\Delta t)$, $\mathbf{x}_{Tr}(3\Delta t)$, ... , can be approximated by the same procedure.

The Newton-Raphson method requires matrix inversion operations. Correspondingly, computational burden can be high when a large number of state variables are not observable in (2.7). However, it is noted that the matrices that need to be inverted here are the Jacobian matrix of $\mathbf{x}_{Tr}(t) + \mathbf{f}_{Tr}[\mathbf{x}_{Tr}(t)] \cdot \Delta t/2$, which equals to $\mathbf{I} + \mathbf{J}_{Tr}[\mathbf{x}_{Tr}(t)] \cdot \Delta t/2$ ($\mathbf{J}_{Tr}[\mathbf{x}_{Tr}(t)]$ is the time-varying Jacobian matrix of $\mathbf{f}_{Tr}(\mathbf{x})$ along with the trajectory $\mathbf{x}_{Tr}(t)$). It is diagonally dominant when Δt is small. Note that by simplifying the matrices as diagonal, the computational burden is dramatically reduced without compromising the accuracy.

2.5.3 Gram-Schmidt Reorthonormalization (GSR)

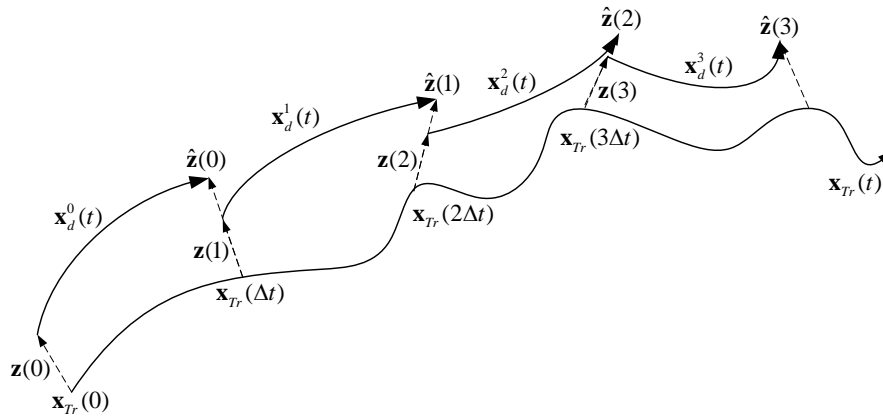


Fig. 2.5. The standard method with GSR

The standard method with GSR [33] is used to calculate $\lambda_{t=T}$ after the estimation of $\mathbf{x}_{Tr}(t)$. The method is based on (2.6), from which one can obtain

$$\lambda \approx t^{-1} \ln[\|\Delta \mathbf{x}(t)\| / \|\Delta \mathbf{x}_0\|] \quad (2.8)$$

The algorithm proceeds as follows:

- 1) Let $\mathbf{z}(0) = (1, 0, 0, \dots)^T$, $j = 0$, and $\lambda^{(-1)} = 0$.
- 2) Do the following while $j \leq T/\Delta t$
 - a. Assume that there is another trajectory $\mathbf{x}_d^j(t)$ of the dynamical system $\frac{d\mathbf{x}}{dt} = \mathbf{f}_{Tr}(\mathbf{x})$ with a different initial point than $\mathbf{x}_{Tr}(0)$. The separation of the two trajectories is $\mathbf{z}(j)$ at $t = j\Delta t$. Then $\mathbf{x}_d^j(j\Delta t) = \mathbf{x}_{Tr}(j\Delta t) + \mathbf{z}(j)$ at $t = j\Delta t$, as shown in Fig. 2.5. Compute the separation $\hat{\mathbf{z}}(j)$ at $t = (j + 1)\Delta t$.

$$\hat{\mathbf{z}}(j) = \mathbf{x}_d^j[(j + 1)\Delta t] - \mathbf{x}_{Tr}[(j + 1)\Delta t] \approx \{\mathbf{I} + \mathbf{J}_{Tr}[\mathbf{x}_{Tr}(j\Delta t)]\Delta t\}\mathbf{z}(j) \quad (2.9)$$

- b. Compute the rate of the separation $\eta^{(j)}$ at that moment.

$$\eta^{(j)} = \ln[\|\hat{\mathbf{z}}(j)\| / \|\mathbf{z}(j)\|] \quad (2.10)$$

- c. Compute the time average of the rate of the separation by $t = (j + 1)\Delta t$.

$$\lambda^{(j)} = \frac{[\eta^{(0)} + \eta^{(1)} + \dots + \eta^{(j)}]}{[(j+1)\Delta t]} = \lambda^{(j-1)} \cdot j/(j + 1) + \eta^{(j)}/[(j + 1)\Delta t] \quad (2.11)$$

- d. Reorthonormalize the separation, so that $\mathbf{z}(j + 1)$ has the same direction that $\hat{\mathbf{z}}(j)$ does, while the magnitude of $\mathbf{z}(j + 1)$ equals to 1, as shown in Fig. 2.5.

$$\mathbf{z}(j + 1) = \hat{\mathbf{z}}(j) \|\mathbf{z}(j)\| / \|\hat{\mathbf{z}}(j)\| \quad (2.12)$$

- e. $j = j + 1$

3) When $j = T/\Delta t + 1$, the time average of the rate of the separation by

$$t = T + \Delta t \text{ equals to } \lambda_{t=T}, \text{ so } \lambda_{t=T} = \lambda^{(j-1)}.$$

2.6 Simulation Results

A 3-machine system and a 200-bus system are used for the validation of the proposed method.

2.6.1 3-machine System

For illustration of the computational techniques, a simple 3-machine system with lossless transmission lines is used, as shown in Fig. 2.6. Classical swing equations are given as follows:

$$\begin{aligned} P_{M1} &= M_1 \ddot{\delta}_1 + D_1 \dot{\delta}_1 + E_1 E_2 / X_{12} \cdot \sin(\delta_1 - \delta_2) + E_1 E_3 / X_{13} \cdot \sin(\delta_1 - \delta_3) \\ P_{M2} &= M_2 \ddot{\delta}_2 + D_2 \dot{\delta}_2 + E_1 E_2 / X_{12} \cdot \sin(\delta_2 - \delta_1) + E_2 E_3 / X_{23} \cdot \sin(\delta_2 - \delta_3) \\ P_{M3} &= M_3 \ddot{\delta}_3 + D_3 \dot{\delta}_3 + E_1 E_3 / X_{13} \cdot \sin(\delta_3 - \delta_1) + E_2 E_3 / X_{23} \cdot \sin(\delta_3 - \delta_2) \end{aligned} \quad (2.13)$$

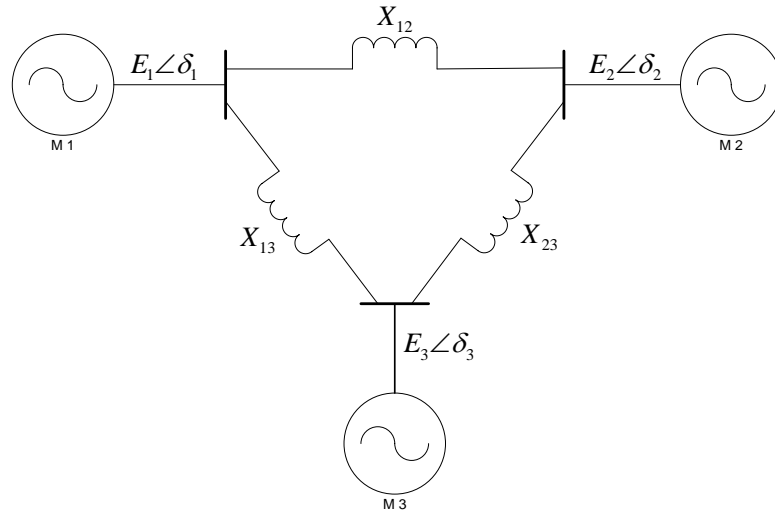


Fig. 2.6. A 3-machine system

In the simulations, it is assumed that $D_1/M_1 = 0.5$, $D_2/M_2 = 0.3$, $D_3/M_3 = 0.2$, $P_{M1}/M_1 = P_{M2}/M_2 = 0.85$, $P_{M3}/M_3 = -1.7$, $E_1 E_2 / M_1 = E_1 E_2 / M_2 = 0.1$, $E_1 E_3 /$

$M_1 = E_1 E_3 / M_3 = E_2 E_3 / M_2 = E_2 E_3 / M_3 = 1.0$. A 6-dimensional dynamical system is obtained:

$$\begin{aligned}
 \dot{\delta}_1 &= \omega_1 \\
 \dot{\omega}_1 &= 0.85 - 0.1 \cdot \sin(\delta_1 - \delta_2) / X_{12} - \sin(\delta_1 - \delta_3) / X_{13} - 0.5\omega_1 \\
 \dot{\delta}_2 &= \omega_2 \\
 \dot{\omega}_2 &= 0.85 - 0.1 \cdot \sin(\delta_2 - \delta_1) / X_{12} - \sin(\delta_2 - \delta_3) / X_{23} - 0.3\omega_2 \\
 \dot{\delta}_3 &= \omega_3 \\
 \dot{\omega}_3 &= -1.7 - \sin(\delta_3 - \delta_1) / X_{13} - \sin(\delta_3 - \delta_2) / X_{23} - 0.2\omega_3
 \end{aligned} \tag{2.14}$$

Assume that $X_{12} = X_{13} = X_{23} = 1$ p.u. A 3-phase fault followed by a normal clearing is applied to each transmission line respectively. The fault is cleared by relay and breaker operations, which will last for a fraction of a second. Then it is assumed that the breaker recloses successfully at 1s. During the fault clearing period, one parameter of the dynamical system in (2.14) is changed since one branch is de-energized. Then the parameter will change back to the original value if the break recloses and it is successful.

Assume that there is one PMU at every generator bus; it is desirable to monitor the real-time values of the state variables in (2.14). The time-varying Jacobian matrix of (2.14) is obtained. Let $\Delta t = 0.01s$, $T = 2s$. $\lambda_{t=2}$ is calculated by the standard method with GSR. $\lambda_{t=2}$ and time-domain simulation results are shown in Table 2.1. As it shows, $\lambda_{t=2}$ predicts losses of synchronism correctly.

Table 2.1. The simulation results of the 3-machine system

3-phase fault	Clearing	Time-domain simulation result	$\lambda_{t=2}$
Branch 1-2	Branch 1-2	stable	-0.0869
Branch 2-3	Branch 2-3	unstable	0.3139
Branch 1-3	Branch 1-3	unstable	0.7823

Note that in the third contingency in Table 2.1, the power swing may appear to be stable based on the observations during the first 3 seconds, but it turns out to be unstable later, as shown in Fig. 2.7. $\lambda_{t=2}$ predicts the instability correctly.

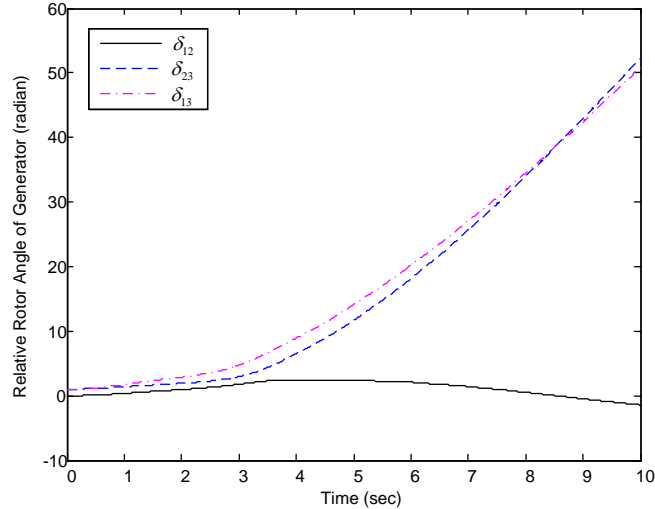


Fig. 2.7. The time-domain simulation result for the 3rd contingency

2.6.2 200-bus System

A 200-bus system that resembles the structure of WECC power grid, as shown in Fig. 2.8, is used for testing of the monitoring algorithm. The model has 31 generators and 8 of them are observable by PMU data. The power system is simulated with PSS/E software tool. Each synchronous machine is modeled as a round-rotor generator and each load is represented by shunt admittance at its bus. The proposed algorithm is implemented in Matlab. It processes the data generated by PSS/E and calculates MLE.

The North American Electric Reliability Corporation (NERC) disturbance class B given in NERC Planning Standards is considered. Here it is condensed to a 3-phase fault for 0.07s with clearing of the related generator or transmission circuit.

Spectrum analysis is performed in off-line study to determine an appropriate time interval for MLE. Time-domain simulations are carried out after NERC disturbance class B. Then spectrum analysis is performed on the resultant power swing curves. It shows that the power swing curves oscillate within 0.2-1.0 Hz. Therefore, T is set as 5s. $\lambda_{t=5}$ is to be calculated to determine angle stability after disturbances.

A 62-dimensional dynamical system model is established to represent the 200-bus system, as shown in Section 2.2. After a disturbance, related parameters of the dynamical system are changed accordingly. 16 state variables of the dynamical system are observed during the contingency period, since only 8 out of 31 generators are observable by PMU data. The other state variables are estimated by the Implicit Integration Method With Trapezoidal Rule, as described in Section 2.5. The approximation results are very close to time-domain simulation results. For example, the relative rotor angle and relative angular speed of the generator at bus 79 after several disturbances are shown in Fig. 2.9. Bus 79 is at the upper left corner of Fig. 2.8, indicated by an oval.

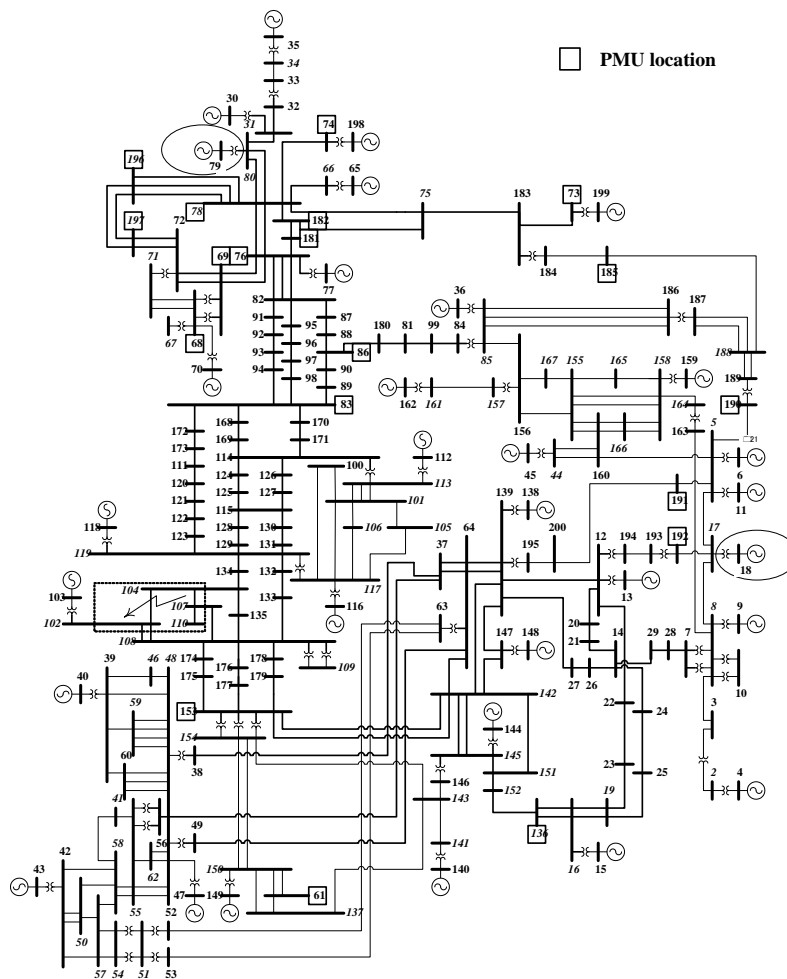


Fig. 2.8. A 200-bus system

After the generator at bus 18 (circled on the right side of Fig. 2.8) is disconnected due to a fault at bus 18, the relative rotor angle and relative angular speed of the generator at bus 79 oscillate dramatically, as Fig. 2.9(a) and (b) show. The approximation results of the angle and relative angular speed coincide with the time-domain simulation results very well. After line 104-102 (marked on the left side of Fig. 2.8) is disconnected, the relative rotor angle and relative angular speed of the generator at bus 79 remain stable, as indicated in Fig. 2.9(c) and (d). The approximation results are reasonable, since the trends of the approximation results coincide well with the time-domain simulation results.

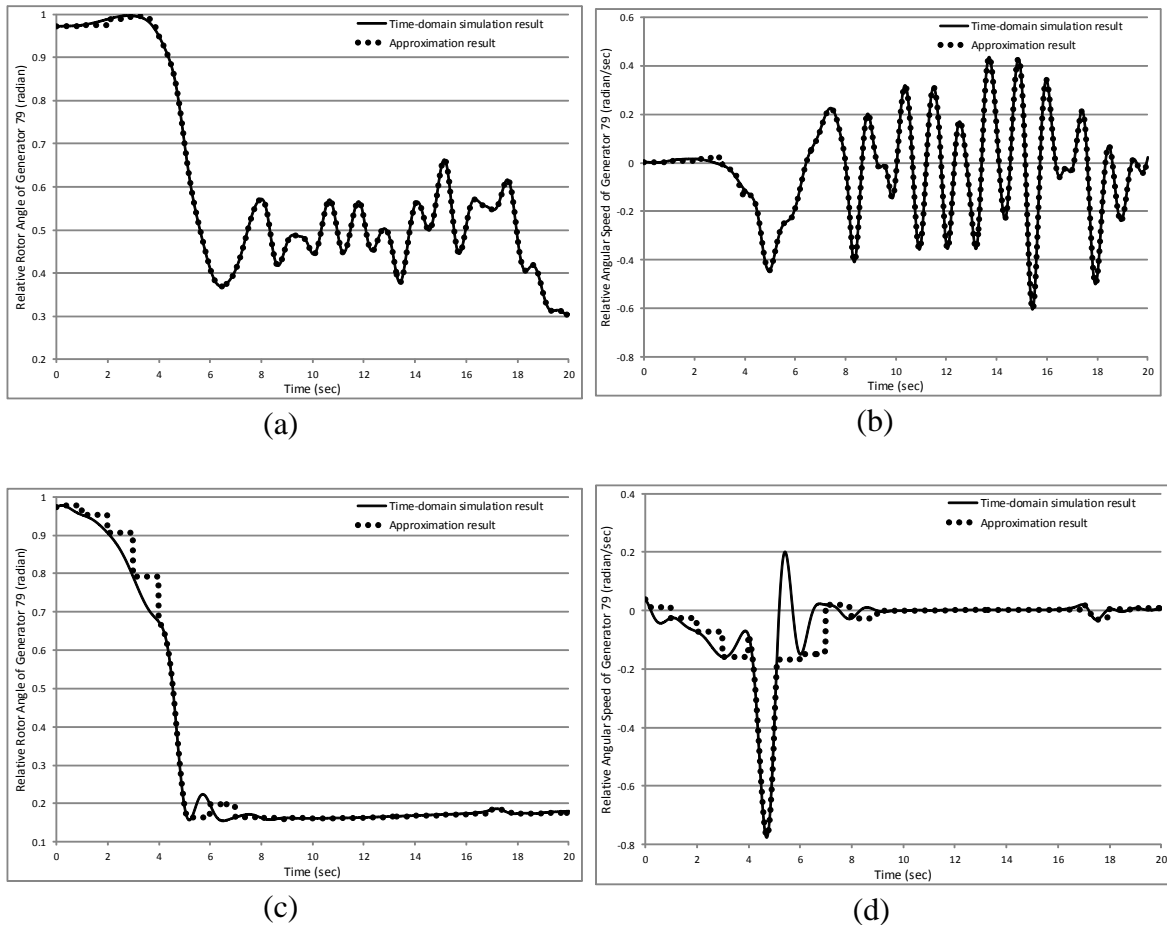


Fig. 2.9. The time-domain simulation results and the approximation results for comparison

The index $\lambda_{t=5}$ is calculated by the standard method with GSR, with all the state variables either observed or estimated. Mechanical power inputs to generators are assumed to keep constant during the calculation of $\lambda_{t=5}$. It is practical because primary controls of generators will not act to change mechanical power inputs until a frequency variation is detected. A detectable frequency variation occurs in swings after the first swing. The calculation of $\lambda_{t=5}$ will be finished before primary controls act. If primary controls do act at some point, system stability will be reassessed. $\lambda_{t=5}$ will be recalculated based on an updated dynamical model.

Table 2.2. The simulation results of the 200-bus system

3-phase fault	Clearing	Time-domain simulation result	$\lambda_{t=5}$
Bus 18	Generator 18	unstable	0.2958
Bus 30	Generator 30	unstable	0.1421
Bus 35	Generator 35	unstable	0.1559
Bus 36	Generator 36	unstable	0.4526
Bus 40	Generator 40	stable	-0.1588
Bus 43	Generator 43	stable	-0.0964
Bus 45	Generator 45	unstable	0.4102
Bus 47	Generator 47	stable	-0.0816
Bus 65	Generator 65	unstable	0.1164
Bus 70	Generator 70	unstable	0.1065
Bus 32	Line 32-31	unstable	0.2782
Bus 64	Line 64-142	stable	-0.1049
Bus 74	Line 74-78	unstable	0.4460
Bus 83	Line 83-168	stable	-0.0434
Bus 104	Line 104-102	stable	-0.3635
Bus 108	Line 108-174	stable	-0.3144
Bus 114	Line 114-171	stable	-0.1026
Bus 119	Line 119-131	stable	-0.1919
Bus 122	Line 122-123	stable	-0.2977
Bus 145	Line 145-151	stable	-0.3150

$\lambda_{t=5}$ and time-domain simulation results for some disturbances are shown in Table 2.2. As shown in the table, $\lambda_{t=5}$ is positive when power swings are unstable after fault clearing; $\lambda_{t=5}$ is negative when power swings are stable.

It is noted that, when the disturbance is generator tripping, the power swing is more likely to be unstable, as Fig. 2.9(a) and (b) show. On the other hand, when the disturbance of line tripping is applied to the power system, the power swing tends to be stable, as illustrated in Fig. 2.9(c) and (d).

Although the unstable cases shown in Table 2.2 are related to the separation of a generator due to a 3-phase bus fault, the 200-bus system, which has a simplified configuration that resembles WECC system, can exhibit complex instability phenomena beyond what is shown by the simulation cases in the research. For example, system oscillations occur after an initiating tree contact with a 500-kV line and the following generator tripping events [34].

2.6.3 Sensitivity Analysis

Table 2.3. The sensitivity analysis results

3-phase fault	Clearing	Time-domain simulation result	$\lambda_{t=3}$	$\lambda_{t=4}$	$\lambda_{t=5}$	$\lambda_{t=6}$	$\lambda_{t=7}$	$\lambda_{t=10}$
Bus 116	Generator 116	unstable	-0.0682	0.1751	0.1368	0.1745	0.1978	0.1748
Bus 138	Generator 138	unstable	0.2119	0.4644	0.4519	0.3234	0.3362	0.1785
Bus 144	Generator 144	unstable	-0.1635	0.1416	0.2172	0.1501	0.1016	0.0778
Bus 149	Generator 149	unstable	0.0620	0.1209	0.2045	0.2679	0.4402	0.4350
Bus 198	Generator 198	unstable	0.2190	0.4344	0.3983	0.2815	0.3320	0.2537
Bus 58	Line 41-58	stable	-0.2327	-0.2199	-0.2066	-0.1890	-0.1545	-0.0220
Bus 142	Line 142-151	stable	-0.2387	-0.2242	-0.2090	-0.1839	-0.1265	-0.1514
Bus 132	Line 132-133	stable	-0.2324	-0.2180	-0.2011	-0.1636	-0.1174	-0.0830
Bus 182	Line 181-182	stable	-0.1450	-0.1401	-0.1353	-0.1306	-0.1255	-0.0862
Bus 155	Line 155-165	stable	-0.1336	-0.1293	-0.1250	-0.1210	-0.1171	-0.1060

A sensitivity analysis with respect to the time interval length T is performed, in

order to quantify its impact on the accuracy of the proposed method. Following a disturbance on the 200-bus system, MLE is calculated over different time windows. Part of the computation results are shown in Table 2.3.

The following facts are observed:

- 1) As the value of T increases, MLE predicts system stability with a higher level of accuracy. For example, $\lambda_{t=3}$ fails to detect instability after the first and third disturbances. MLE calculated over a longer time window provides a correct prediction.
- 2) The value of MLE varies after different disturbances. It is reasonable because different disturbances change power system configurations in different ways, as shown in Table 2.3. Consequently, MLE is calculated based on different dynamical system configurations.
- 3) When the system is unstable, the value of MLE changes with respect to the time interval length T in a pattern that exhibits varying characteristics. This is the case because MLE is calculated based on a nonlinear system trajectory within one time window. When the nonlinear system is unstable, small changes in the time window length T can cause the value of MLE to vary significantly.
- 4) When the system is stable, the value of MLE is negative but tends to increase as the window size increases, as shown in Table 2.3. The observation seems to indicate that the system is considered less stable when a larger set of observations are obtained by a wider time window. For a power system undergoing a contingency, it is reasonable that more

variations are observed within a larger time frame.

2.6.4 Computational Burden

The total computational burden of the proposed algorithm is affordable for on-line applications. Consider a power system with n_1 generators, n_2 of which are not observed by PMU data. If $\Delta t = 0.01s$, $T = 5s$, and the Newton-Raphson method iterates 20 times at most, the main computational burden would be $500 * (2n_1^2 + 3n_1) + 100000n_2$ multiplication operations and $500 * (n_1^2 + 2n_1) + 130000n_2$ addition operations. Taking the 200-bus system in Subsection 2.6.2 as an example; it takes 0.0044 sec to calculate $\lambda_{t=5}$ for a 3 GHz Pentium 4 CPU. Moreover, the proposed algorithm is recursive. It does not have to obtain all the PMU data needed before calculating MLE. For example, if $\lambda_{t=5}$ is to be calculated, and PMUs transmit 1-sec time window data every time, the algorithm can start calculating once the first 1-sec time window data is obtained, and wait for the next one from PMUs at the same time.

2.7 Discussion

A PMU-based method for on-line dynamic security assessment has been developed. The main idea is to calculate MLE in order to predict a loss of synchronism. The proposed MLE method is based on a solid analytical foundation, and it is computationally efficient.

CHAPTER 3. RISK ASSESSMENT FOR CYBER SECURITY

3.1 State-of-the-art

In 2006, US Department of Energy (DOE) published “Roadmap to secure control systems in the energy sector” (updated in 2011) [35]. It envisions that: in 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of any critical function. Much effort has been made to secure the facilities. The DOE National SCADA Test Bed (NSTB) Program, established in 2003, supports industry and government efforts to enhance cyber security of control systems in the energy sector. The NERC standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of critical cyber assets to support reliable operations of the bulk electric system [36]. The International Electrotechnical Commission Technical Council (IEC TC 57), i.e., power system management and associated information exchange, has advanced the standard communication protocol security in IEC62351 with stronger encryption and authentication mechanisms [37]. The Hallmark Project by Schweitzer Engineering Laboratories, Inc. presents the Secure SCADA Communications Protocol (SSCP) technology which provides integrity for SCADA messages. United States Computer Emergency Readiness Team (US-CERT) has set up awareness programs about system vulnerabilities to improve control system security [38]. The Cyber Security Audit and Attack Detection Toolkit by Digital Bond, Inc. is developed to identify vulnerable configurations in control system devices and applications. Reference [39] presents a risk assessment methodology that accounts for both physical and cyber security of critical infrastructures. In [40], a SCADA security framework is proposed. System vulnerabilities

are assessed quantitatively through an attack tree. The impact of a cyber attack on SCADA systems is studied systematically in [41]. It is evaluated by the resultant loss of load through a power flow computation.

This research presents a new risk assessment framework for SCADA systems of power grids. Individual vulnerabilities within control systems are evaluated based on the Duality Element Relative Fuzzy Evaluation Method (DERFEM). An attack graph is developed to identify possible intrusion scenarios that exploit multiple security vulnerabilities. An Intrusion Response System (IRS) based on PMU data is proposed to assess the impact of intrusion scenarios on power system dynamics.

The main contribution is IRS, which is an on-line monitoring and control scheme based on PMUs. It monitors the impact of cyber intrusions on power system dynamics in real time. If power system instability such as voltage instability is judged to be likely after a cyber attack, IRS will act as a mitigation mechanism to prevent power system instability. Unlike traditional security mechanisms such as encryption and authentication, which increase the complexity of power systems, and may cost additional time in power system operations, IRS uses a control strategy based on the Conditional Lyapunov Exponents (CLEs) to enhance the resilience of power systems against cyber attacks.

3.2 Risk Assessment Framework

The risk assessment framework is shown in Fig. 3.1. For SCADA systems of a power system, the procedure starts with identification of the configuration of its cyber system. The vulnerabilities within the cyber system are then identified. Each vulnerability is evaluated quantitatively by DERFEM. An attack graph is built to identify possible intrusion scenarios that exploit multiple vulnerabilities. The probability of occurrence of

every intrusion scenario is calculated. Once an intrusion scenario is successfully executed, IRS will monitor its impact on power system dynamics in real time. The impact is characterized by CLEs computed on PMU data. If values of CLEs are high, it is judged that voltage instability is likely to happen. Control actions based on CLEs will be taken to prevent voltage instability.

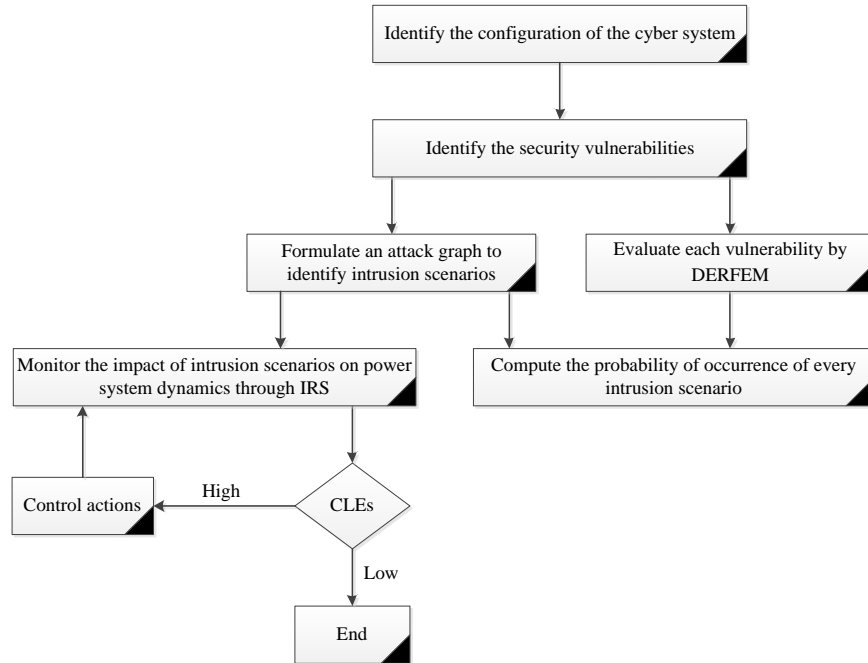


Fig. 3.1. The proposed risk assessment framework

3.2.1 Duality Element Relative Fuzzy Evaluation Method

Suppose that a cyber system has n identified vulnerabilities: r_1, r_2, \dots, r_n . DERFEM is employed to assign each vulnerability a scaled value within $[0, 1]$ which quantitatively characterizes the vulnerable level. The larger the scaled value is; the higher the vulnerable level will be.

DERFEM proceeds as follows:

- 1) Compare a pair of different vulnerabilities (r_i, r_j) so as to obtain the scaled

values $Com_{r_j}(r_i)$ and $Com_{r_i}(r_j)$. $Com_{r_j}(r_i)$ represents the vulnerable level of r_i compared to r_j . Likewise, $Com_{r_i}(r_j)$ represents the vulnerable level of r_j compared to r_i . $0 \leq Com_{r_j}(r_i) \leq 1$; $0 \leq Com_{r_i}(r_j) \leq 1$. If $Com_{r_j}(r_i) > Com_{r_i}(r_j)$, it implies that the vulnerability r_i has a higher vulnerable level than r_j does.

- 2) Continue the comparison of different pairs of individual vulnerabilities until a matrix such as Table 3.1 is generated ($Com_{r_i}(r_i)$ is set to be 1 here for convenience of the calculation).
- 3) In each row of Table 3.1, substitute $Com_{r_j}(r_i)$ with $Com(r_i/r_j)$, where $Com(r_i/r_j) = Com_{r_j}(r_i) / \max[Com_{r_j}(r_i), Com_{r_i}(r_j)]$.
- 4) Finally, the vulnerable level of r_i is quantitatively characterized by $Vul(r_i)$; $Vul(r_i) = \min[Com(r_i/r_1), Com(r_i/r_2), \dots, Com(r_i/r_n)]$.

Table 3.1. The comparison results of the vulnerabilities

	r_1	r_2	r_3	...	r_n
r_1	1	$Com_{r_2}(r_1)$	$Com_{r_3}(r_1)$...	$Com_{r_n}(r_1)$
r_2	$Com_{r_1}(r_2)$	1	$Com_{r_3}(r_2)$...	$Com_{r_n}(r_2)$
r_3	$Com_{r_1}(r_3)$	$Com_{r_2}(r_3)$	1	...	$Com_{r_n}(r_3)$
\vdots	\vdots	\vdots	\vdots	\ddots	\vdots
r_n	$Com_{r_1}(r_n)$	$Com_{r_2}(r_n)$	$Com_{r_3}(r_n)$...	1

DERFEM does not measure the vulnerable level of vulnerability directly, which could be difficult. It reveals the relatively vulnerable level of the vulnerability compared to the others.

3.2.2 Attack Graph

In practice, a hacker may have to compromise a couple of interconnected hosts within a cyber system before he/she gains access to the control systems. For example, an

outside intruder has to compromise an enterprise network, and then attack the connected industrial control systems via the enterprise network. This procedure is modeled as an intrusion scenario in this research. An intrusion scenario is comprised of several intrusion actions; each action involves exploiting one security vulnerability.

An attack graph is employed to capture possible intrusion scenarios within a cyber system. The attack graph depicts ways in which a hacker compromises the interconnected hosts sequentially by exploiting the corresponding vulnerabilities so as to achieve a specific goal. The benefits of the attack graph takes into account the effects of interactions of local vulnerabilities and find global security holes introduced by the interconnections [42].

The basic concepts of the attack graph are defined as follows.

Definition 3.1: Subject (ST). Subject is the initiator of actions. $st \in ST$ can be an attacker or a compromised device.

Definition 3.2: Node (ND). An electronic device in a cyber system is a node, using $nd = (id), nd \in ND$ to denote. id is the identifier of the node, and it could be set as an equipment name. If a node is compromised by a subject, the node itself will become a subject.

Definition 3.3: Privilege (PG). It is used to describe the operating privilege of a subject in a node. When $st \in ST$ and $nd \in ND$, the function $pg(st, nd) \rightarrow \{0,1,2,3,4,5\}$ expresses the privilege level of st in nd . $pg(st_i, nd_j) = 0$ implies that Subject st_i has no access to Node nd_j ; $pg(st_i, nd_j) = 1$ indicates that Subject st_i is able to read the inbound and outbound messages of Node nd_j ; $pg(st_i, nd_j) = 2$ means that Subject st_i is able to block the inbound and outbound messages of Node nd_j ; $pg(st_i, nd_j) = 3$

represents that Subject st_i can read and block the inbound and outbound messages of Node nd_j ; $pg(st_i, nd_j) = 4$ denotes that Subject st_i can send messages to Node nd_j ; $pg(st_i, nd_j) = 5$ signifies that Subject st_i has the full control access to Node nd_j .

Definition 3.4: State (Z). State is a triple $z = [st, nd, pg(st, nd)]$. State is the prerequisite of the next attack action to be implemented.

Definition 3.5: Interconnection (IC). Interconnection refers to connections between nodes, using a quadruplet $ic = (nd_i, nd_j, ch_{ij}, mt_{ij})$, $ic \in IC$, $nd_i, nd_j \in ND$ to denote. ch_{ij} represents the communication channel between nd_i and nd_j . ch_{ij} could be copper wires, optical fibers, wireless, Dial-up, Virtual Private Network (VPN), or digital microwave. mt_{ij} is the type of the messages from nd_i to nd_j . mt_{ij} could be measurements or control signals. mt_{ij} does not necessarily equal to mt_{ji} .

Definition 3.6: Action (A). Action represents the set of possible actions of the subjects in a cyber system. Action is a quadruplet $a = (name, z_s, z_d, r)$, $a \in A$, $z_s, z_d \in Z$. $name$ is the name of the attack action such as the Denial-of-Service (DOS) attack and the man-in-the-middle attack; z_s and z_d represent the initial state and final state of the action; r is the vulnerability exploited in the action. r is used to denote the difficult level of Action a .

The algorithm to construct an attack graph proceeds as follows:

- 1) Identify ND and IC . Develop a directed graph (ND, IC) . The vertex is $nd \in ND$, and the edge is $ic \in IC$.
- 2) Identify the nodes nd_{t_i} which will be the targets of attacks. nd_{t_i} could be a SCADA server or a Programmable Logic Controller (PLC).
- 3) Determine the goals of attacks – the state of nd_{t_i} after being attacked,

formulated as follows: $z_d = [st_0, nd_{t_i}, pg(st_0, nd_{t_i}) > 0]$, where st_0 represents the initial intruding subject (hackers).

- 4) Traverse the directed graph (ND, IC). Identify the nodes nd'_{t_i} that are connected to nd_{t_i} directly. Assume that Node nd'_{t_i} has been compromised by st_0 , and it becomes an intruding subject, say st'_{t_i} .
- 5) Extract an attack action aimed at nd_{t_i} from st'_{t_i} , such that $a = (name, z_s, z_d, r_a)$, $z_d = [st'_{t_i}, nd_{t_i}, pg(st'_{t_i}, nd_{t_i}) = pg(st_0, nd_{t_i})]$. r_a is the vulnerability of Node nd_{t_i} exploited in Action a .
- 6) Establish the prerequisite of Action a : z_s , formulated as follows: $z_s = [st_0, nd'_{t_i}, pg(st_0, nd'_{t_i}) > 0]$.
- 7) Set nd'_{t_i} as a new target node, and z_s becomes another z_d . Repeat Step 4, 5 and 6, until $st'_{t_i} = st_0$.

After the attack graph is built, it gives a bird's-eye view of possible intrusion scenarios. For each scenario, the probability of occurrence *Prob* is calculated as follows:

- If the intrusion scenario is comprised of two serial intrusion actions a_i and a_j , then

$$Prob = Vul(r_{a_i}) \times Vul(r_{a_j}) \quad (3.1)$$

where r_{a_i} and r_{a_j} are the local vulnerabilities exploited in the attack actions a_i and a_j .

- If the intrusion scenario consists of two parallel intrusion actions a_i and a_j , then

$$Prob = Vul(r_{a_i}) + Vul(r_{a_j}) - Vul(r_{a_i}) \times Vul(r_{a_j}) \quad (3.2)$$

- If the intrusion scenario is more complicated, the calculation of its *Prob* will be the synthesis of (3.1) and (3.2).

3.2.3 Intrusion Response System

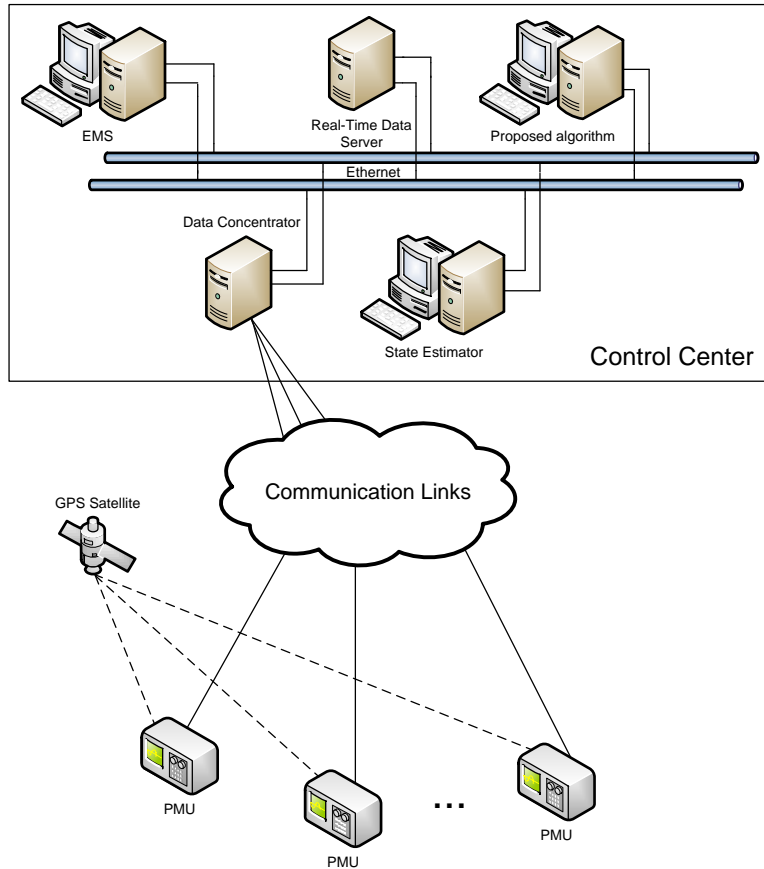


Fig. 3.2. Concept of IRS

The concept of IRS is illustrated in Fig. 3.2. It is intended to be an application in the control center of a power system. The proposed algorithm, which will be discussed in detail in Section 3.3, obtains updated power network configurations from the State Estimator (SE), say, every 5 minutes. If an intrusion scenario is executed successfully, and it results in disruptions in power system operations such as breaker opening and loss of generation, such sudden changes of power network configurations will be reported to

the propose algorithm through SCADA systems in real time. The post-attack dynamical model of the power system is then built. After that, the algorithm extracts synchronized phasor measurements from the PMU data concentrator, which obtains real time PMU data from substations equipped with PMUs. Hence, a number of the state variables of the dynamical model are observed from PMU data. Based on the dynamical model and PMU measurements, CLEs are calculated to monitor the impact of an intrusion on power system dynamics.

If CLEs only have low values, the prediction is that voltage instability will not happen; otherwise, voltage instability is likely to occur, and the proposed algorithm will send proper control signals to the Energy Management System (EMS) to prevent voltage instability.

3.3 Proposed Algorithm

3.3.1 Dynamical Model

In this algorithm, generators are represented by classical models, and loads are represented by ZIP models. After a cyber intrusion, the dynamical model of a power system (n bus and m generators) is established as shown below:

$$\begin{aligned} \mathbf{Y}_{bus} \dot{\mathbf{V}} &= \mathbf{I} \\ -\dot{V}_i \dot{I}_i^* &= P_{D,i} + jQ_{D,i} \\ \dot{V}_j \dot{I}_j^* &= \dot{V}_j \left(\frac{E_j \angle \delta_j - \dot{V}_j}{Z_j} \right)^* \end{aligned} \quad (3.3)$$

$$\begin{aligned} \frac{d\delta_j}{dt} &= \omega_j \\ \frac{2H_j}{\omega_{Re}} \frac{d\omega_j}{dt} + \frac{D_j}{\omega_{Re}} \omega_j &= P_{m,j} - \text{Re}(E_j \angle \delta_j \times \dot{I}_j^*) \end{aligned} \quad (3.4)$$

where $i = 1, 2, \dots, n - m$, and $j = n - m + 1, \dots, n$. δ_j is the rotor angle of generator j , ω_j is the angular speed, and $P_{D,i} + jQ_{D,i}$ is the power consumption at load bus i . $P_{D,i} =$

$$P_{0,i} \left\{ A_i + B_i \left(\frac{|V_i|}{|V_{0,i}|} \right) + C_i \left(\frac{|V_i|}{|V_{0,i}|} \right)^2 \right\} (1 + L_{P,i} \Delta f) \quad ; \quad Q_{D,i} = Q_{0,i} \left\{ D_i + E_i \left(\frac{|V_i|}{|V_{0,i}|} \right) + F_i \left(\frac{|V_i|}{|V_{0,i}|} \right)^2 \right\} (1 + L_{Q,i} \Delta f). \Delta f \text{ is the system frequency deviation in per unit.}$$

Excitation systems of generators are assumed to function in some way to keep internal voltage magnitudes at some reference values during a transient period. The time constant of modern excitation systems is less than 0.5s. If a new reference value is issued to an excitation system, the corresponding voltage magnitude will change rapidly due to the fast response of the excitation system. MCLEs will be computed based on an updated dynamical model to reassess system stability.

Let \mathbf{x} denote $[|V_1|, \angle V_1, |V_2|, \angle V_2, \dots, |V_n|, \angle V_n]^T$, and \mathbf{y} denote $[\delta_1, \omega_1, \dots, \delta_m, \omega_m]^T$. (3.3) and (3.4) are represented by:

$$\mathbf{G}(\mathbf{x}, \mathbf{y}) = 0 \quad (3.5)$$

$$\frac{d\mathbf{y}}{dt} = \mathbf{F}(\mathbf{x}, \mathbf{y}) \quad (3.6)$$

Since

$$\frac{d\mathbf{G}(\mathbf{x}, \mathbf{y})}{dt} = 0 = \mathbf{G}_x \frac{d\mathbf{x}}{dt} + \mathbf{G}_y \frac{d\mathbf{y}}{dt} \quad (3.7)$$

It is obtained that

$$\frac{d\mathbf{x}}{dt} = -(\mathbf{G}_x)^{-1} \mathbf{G}_y \frac{d\mathbf{y}}{dt} = -(\mathbf{G}_x)^{-1} \mathbf{G}_y \mathbf{F}(\mathbf{x}, \mathbf{y}) \quad (3.8)$$

where \mathbf{G}_x (resp. \mathbf{G}_y) denotes the Jacobian matrix of \mathbf{G} with respect to \mathbf{x} (resp. \mathbf{y}). When $\det(\mathbf{G}_x) = 0$ and $\mathbf{G}_y \frac{d\mathbf{y}}{dt} \neq 0$, $\frac{d\mathbf{x}}{dt}$ has very large values. Correspondingly, the voltages \mathbf{x} will change dramatically, and voltage instability is likely to happen.

3.3.2 Methodology: Conditional Lyapunov Exponents

The notion of CLEs (originally called Sub-Lyapunov Exponents) is introduced by Pecora and Carroll in their study of synchronization of chaotic systems [43] and [44]. Similar to the full Lyapunov Exponents, CLEs are well defined ergodic invariants.

Consider a N -dimensional continuous-time dynamical system $\frac{dz}{dt} = \mathbf{H}(\mathbf{z})$. If one split the state vector \mathbf{z} into two vectors: $\mathbf{z}_1 \in R^K$, and $\mathbf{z}_2 \in R^{N-K}$ ($0 < K < N$), one will obtain two sub systems: $\frac{dz_1}{dt} = \mathbf{H}_1(\mathbf{z}_1, \mathbf{z}_2)$ and $\frac{dz_2}{dt} = \mathbf{H}_2(\mathbf{z}_1, \mathbf{z}_2)$. Let $\mathbf{z}_1(t) = \boldsymbol{\varphi}(t, \mathbf{v}_1, \mathbf{v}_2)$ be the solution of the first sub system at time t starting from the initial conditions $\mathbf{z}_1^0 = \mathbf{v}_1$, $\mathbf{z}_2^0 = \mathbf{v}_2$. The Conditional Lyapunov Exponents CLE_i for the sub system $\frac{dz_1}{dt} = \mathbf{H}_1(\mathbf{z}_1, \mathbf{z}_2)$ are defined as eigenvalues of the following limiting.

$$\begin{aligned} \Lambda(\mathbf{v}_1) &= \lim_{t \rightarrow \infty} [\mathbf{K}^T(t, \mathbf{v}_1, \mathbf{v}_2) \mathbf{K}(t, \mathbf{v}_1, \mathbf{v}_2)]^{1/2t} \\ CLE_i(\mathbf{v}_1) &= \ln[\bar{\lambda}_i(\mathbf{v}_1)] \end{aligned} \quad (3.9)$$

where $i=1,2,\dots,K$. $\mathbf{K}(t, \mathbf{v}_1, \mathbf{v}_2)$ is the Jacobian matrix of $\boldsymbol{\varphi}(t, \mathbf{v}_1, \mathbf{v}_2)$ with respect to \mathbf{v}_1 , and $\bar{\lambda}_i(\mathbf{v}_1)$ is the i th eigenvalue of $\Lambda(\mathbf{v}_1)$. The existence of CLEs is guaranteed under the same conditions that establish the existence of the Lyapunov Exponents [45].

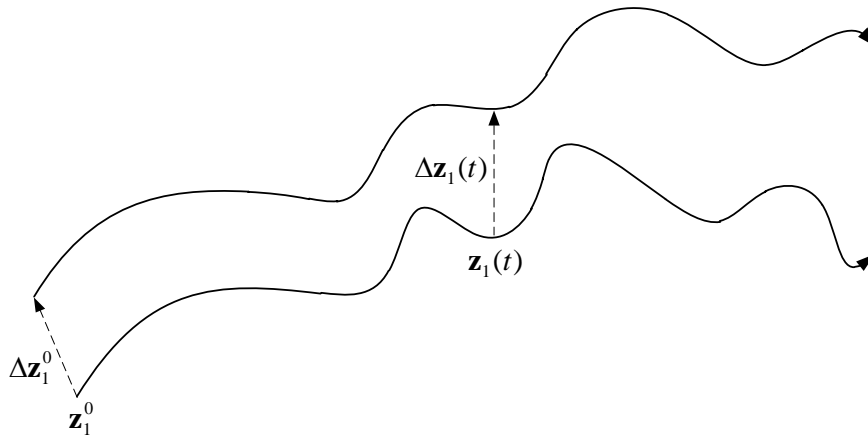


Fig. 3.3. Nearby trajectories in the state space

The relationship between CLEs and system stability is discussed in the following. In ergodic theory of dynamical systems, the Lyapunov Exponents are used to characterize the exponential divergence or convergence of nearby trajectories, as shown in Fig. 3.3. For the sub system $\frac{dz_1}{dt} = \mathbf{H}_1(\mathbf{z}_1, \mathbf{z}_2)$, its Maximal Conditional Lyapunov Exponent (MCLE) determines the exponential convergence of nearby system trajectories. This is true due to the approximation of

$$\|\Delta \mathbf{z}_1(t)\| \approx e^{MCLE \times t} \|\Delta \mathbf{z}_1^0\| \quad (3.10)$$

If $\frac{dz_1}{dt}$ has very large values, the nearby system trajectories will diverge. Correspondingly, $MCLE \gg 0$. Otherwise, the nearby trajectories will converge, and MCLE has a low or even negative value. Therefore, the value of MCLE reveals the magnitude of time derivatives of related state variables. When the state variables are voltages of a power system, MCLE can be used to monitor the magnitude of time derivatives of the voltages, and hence voltage stability.

3.3.3 Application of MCLE

In this work, the dynamical system in (3.8) is split into n sub systems. The i th sub system has the state variables $[|V_i|, \angle V_i]^T$, where $i=1, 2, \dots, n$. MCLE is computed for each sub system to monitor voltage stability within it.

Let $\mathbf{G}_y \frac{dy}{dt} = \Phi \in R^{2n}$, one may obtain

$$\Phi_{2i-1} = \frac{|V_i|E_i \cos[\angle(V_i + Z_i - \delta_i)] d\delta_i}{|Z_i|} \frac{d\delta_i}{dt} + Q_{0,i} \left\{ D_i + E_i \left(\frac{|V_i|}{|V_{0,i}|} \right) + F_i \left(\frac{|V_i|}{|V_{0,i}|} \right)^2 \right\} L_{Q,i} \frac{d\Delta f}{dt}$$

$$\Phi_{2i} = -\frac{|V_i|E_i \sin[\angle(V_i + Z_i - \delta_i)] d\delta_i}{|Z_i|} \frac{d\delta_i}{dt} + P_{0,i} \left\{ A_i + B_i \left(\frac{|V_i|}{|V_{0,i}|} \right) + C_i \left(\frac{|V_i|}{|V_{0,i}|} \right)^2 \right\} L_{P,i} \frac{d\Delta f}{dt}$$

where $i=1,2,\dots,n$. $E_i = 0$, $|Z_i| = \infty$, and $\delta_i = 0$, if there is no generator at bus i . As $\frac{d\Delta f}{dt}$ is small,

$$\Phi_{2i-1} \approx \frac{|V_i|E_i \cos[\angle(V_i + Z_i - \delta_i)]}{|Z_i|} \omega_i$$

$$\Phi_{2i} \approx -\frac{|V_i|E_i \sin[\angle(V_i + Z_i - \delta_i)]}{|Z_i|} \omega_i$$

One can assume that \mathbf{G}_x is diagonal in computation without compromising the accuracy, and then the i th sub system of (3.8) is represented by

$$\begin{aligned} \frac{d|V_i|}{dt} &= -\frac{\Phi_{2i-1}}{\mathbf{G}_x(2i-1,2i-1)} \\ \frac{d\angle V_i}{dt} &= -\frac{\Phi_{2i}}{\mathbf{G}_x(2i,2i)} \end{aligned} \quad (3.11)$$

where $i=1,2,\dots,n$. $\mathbf{G}_x(i,j)$ is the element at the i th row and j th column of \mathbf{G}_x . It is noted that $\frac{d|V_i|}{dt} = \frac{d\angle V_i}{dt} = 0$ if there is no generator at bus i , which is reasonable since the change of voltages at the load buses is driven by voltages at the generator buses. Consequently, $\frac{d|V_i|}{dt}$ and $\frac{d\angle V_i}{dt}$ do not depend on $|V_i|$ and $\angle V_i$.

The proposed algorithm calculates MCLEs of the sub systems that have generators at the corresponding buses. The computation method is introduced in the following.

3.3.4 Computation Method

MCLEs are calculated over a limited time window. PMU measurements are extracted to observe time-varying values of the state variables of the sub systems. The unobservable part of the state variables is approximated through the Implicit Integration Method With Trapezoidal Rule in Subsection 2.5.2. The algorithm in Subsection 2.5.3,

the standard method with GSR, is then used to compute MCLEs. If values of MCLEs are over a predefined limit, it is predicted that voltage instability will happen. Control signals will be sent to EMS and initiate actions to prevent voltage instability.

Selection of the length of time interval could be arbitrary. Study shows that MCLEs exhibit robustness to the length of time interval: MCLEs computed over different length time intervals all have very high values if voltage instability is going to happen. In this research, the time interval length is set to be 0.2s, so that it is short while it has enough PMU measurements.

3.3.5 Control Actions

When the value of MCLE of a sub system is over a predefined limit which is much greater than zero, the proposed algorithm will send a control signal to the excitation system of the generator related to the sub system through EMS. The reference value of the generator internal voltage magnitude is modified as follows:

$$E_{Gen}^{ref,new} = (1 + MCLE/const)E_{Gen}^{ref,old} \quad (12)$$

where *const* is a predefined constant value. Voltage instability can be prevented with the fast response of the exciting system.

3.4 Case Study

Wind farm SCADA systems are selected for case study due to the fact that wind power is a fast emerging renewable resource on power grids, and it has the potential to affect the dynamical performance of power systems.

Installed wind power capacity is increasing rapidly in recent years. The year 2008 is a record year for wind generation in US with a total increase of 8,360 MW which is 50% of the total wind capacity at the end of 2007 [46]. Wind energy accounts for 42% of

the total new capacity added. Report [47] from DOE anticipates that wind could power 20% of U.S. grid by 2030.

The increased and concentrated penetration of wind power makes the power network more dependent on wind energy production. Moreover, the newly installed large wind farms will be connected directly to high voltage transmission grids. Until recently, wind farms have been connected to the distribution system, which typically has either 10/20 kV or 50/60 kV grids [48]. This situation means that future wind farms will be able to replace conventional power stations, and thus be active controllable elements in the power supply network. In other words, wind farms must be enabled with the control capabilities of a power plant [49].

The dynamic performance of power systems can be affected by wind farm operations. Cyber attacks on SCADA systems of wind farms present a potential threat for power system stability. There are special concerns for cyber security of wind power. Conventional generation is located in a facility that is at least somewhat secure physically, i.e., it probably has a fence and maybe even security guards. However, anybody can walk up to a wind turbine and knock on the door.

3.4.1 Wind Farm SCADA Systems

The generic network configuration of wind farm SCADA systems is identified and shown in Fig. 3.4. Every wind turbine is equipped with the Wind Turbine Control Panel (WTCP), which monitors and controls the wind turbine. WTCP is normally mounted in the tower base and is easily accessible. Through WTCPs, servers in a control room support monitoring and control of the wind turbines within a wind farm. However the control room is normally not staffed and it is only for maintenance occasions. Wind

farms in separated locations are integrated into a single EMS in a main control center through a control WAN. In a room that looks alike NASA Mission Control, system analysts oversee every turbine at the wind farms. The control center interfaces restrictively with corporate networks for business and operational reasons.

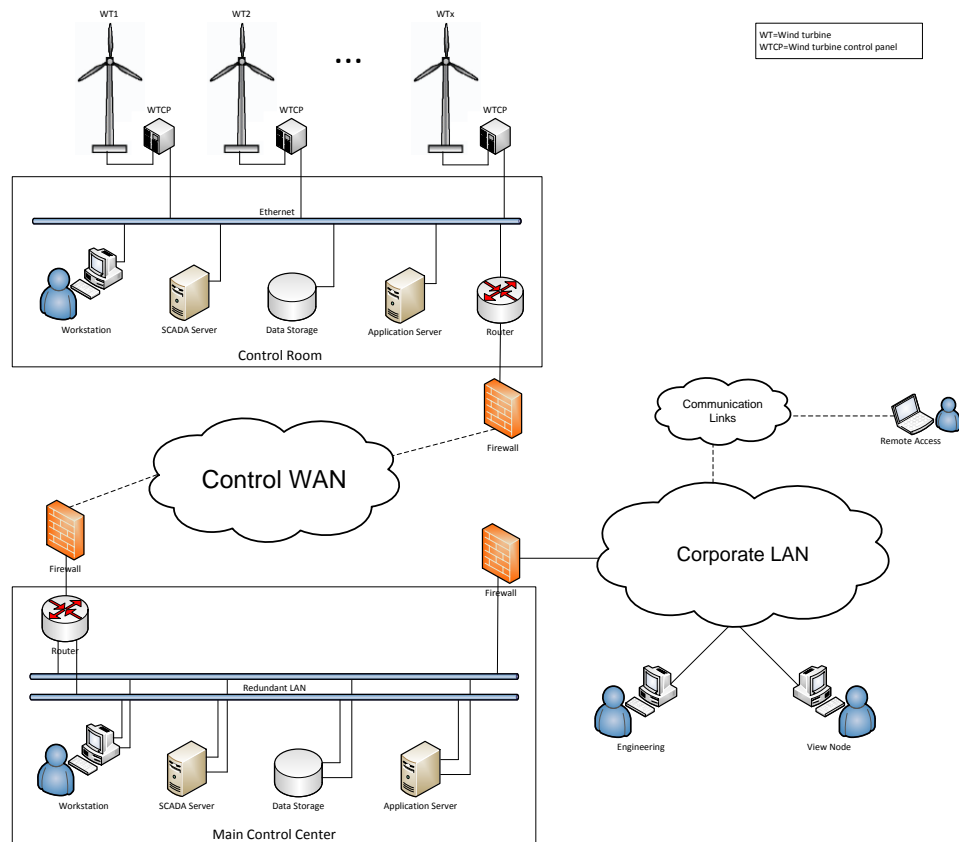


Fig. 3.4. The generic network configuration of wind farm SCADA systems

3.4.2 Security Vulnerabilities

12 vulnerabilities are identified within the generic network configuration of wind farm SCADA systems. The vulnerabilities are illustrated in the following.

Configuration management of WTCPs (r_1)

WTCP has the capability to change configuration settings of a wind turbine. It must support authentication for configuration updates as required by NERC CIP series. In

practice, it is generally equipped with a hardware token based or username-password based authentication [50].

The configuration management is questionable. WTCP is built on open ground, and it could be accessed by unauthorized individuals to gain physical access. Even though WTCP supports some user authentications such as a pin, the pin may be cracked.

A pin can be cracked by a brute force attack. For example, if the key length of the pin is 6, there will be 10^6 possible pins. The brute force attack will traverse the search space of possible pins until a correct one is found. There are a few techniques to help significantly reduce the search space. Hackers can try the initial factory password and some simplistic passwords, as people tend to use those passwords for pins. Hackers may also scan fingerprints on the pin pad left by authorized users. In the best-case scenario, hackers are able to identify the 6 keys of a 6-digit pin, which will reduce the possible pins to 720.

The chemical combinatorial attack in [51] could be used to identify a pin directly. The attack consists in depositing on each pin pad key a small ionic salt quantity (e.g. some NaCl on key 0, some KCl on key 1, LiCl on key 2, SrCl₂ on key 3, BaCl₂ on key 4, CaCl₂ on key 5...). As a user enters his or her pin, salts are mixed and leave the pin pad in a state where secret information can be leaked. The next phase of the attack includes collecting samples from the pin pad and analyzing these using a mass spectrometer. The attack is illustrated in Fig. 3.5 for PIN 1592.

The chemical combinatorial attack could be dangerous for WTCPs. Unlike ATMs, only a few users such as maintenance personnel operate WTCPs, and they do not do it frequently. During a chemical combinatorial attack, the salts on a pin pad would not

be mixed evenly, and therefore give a clear hint of the pin.


1 c_1	2 c_2	3 c_3		1 c_1	2 c_2, c_9, c_5, c_1	3 c_3
4 c_4	5 c_5	6 c_6		4 c_4	5 c_5, c_1	6 c_6
7 c_7	8 c_8	9 c_9		7 c_7	8 c_8	9 c_9, c_5, c_1
* c_0	0 c_0	#		* c_0	0 c_0	#

Fig. 3.5. A chemical combinatorial attack

Implicit trust between WTCPs and a control room (r_2)

The NERC Control System Security Working Group summarizes the problem of implicit trust exceptionally well on their website:

Control systems are the “brains” of control and monitoring of the bulk electric system and other critical infrastructures, but they were designed for functionality and performance, not security. Most control systems assume an environment of complete and implicit trust.

SCADA systems of wind farms operate in an environment of complete and implicit trust. The international standard IEC 61400-25: Communications for monitoring and control of wind power plants specifies data formats and information exchange methods for wind farms. IEC 61400-25 does not support any mechanism to authenticate and validate communication between wind turbines and a control room. It is left to the implementation of IEC 61400-25 to employ security mechanisms. Hence, SCADA systems could be influenced by injected traffic.

Implicit trust between control rooms and a control center (r_3)

The implicit trust between control rooms and a control center is assumed when

the control WAN between them is a private utility Intranet.

Wireless network (r₄)

Wireless technology is considered for SCADA systems of wind farms. The reasons are:

- 1) Wireless technology has the advantages of reduced cost, flexibility of configuration, and ease of maintenance.
- 2) Wireless network can be deployed in a tough terrain where wired infrastructure is difficult to install.
- 3) Wireless communication could be used as a back-up for wired cables to ensure continuity of operations when the wired cables are broken or under attack.

One example of wireless communication architecture for wind farms can be found in [52].

Wireless network is subject to common attacks including sniff, spoof, the man-in-the-middle attack and DoS attack. Even if strong encryption and authentication are applied, wireless communication can still be affected by a jamming attack.

A jamming attack occurs when a hacker analyzes the signal spectrum being used by a wireless network and then transmits a powerful signal to interfere with the communication on the discovered frequencies. A jamming attack is easy to implement in practice. For example, a Bluetooth device located within ten meters of an 802.11b network will cause a jamming. The jamming attack could force the wireless network to hold the transmissions until the disruptive signal no longer exists, or switch to a slower data transmission rate since data needs to be retransmitted from time to time.

Optical fibers (r5)

Optical fibers are used heavily in communication infrastructures of wind farms. Optical fibers are glass or plastic that allows the propagation of light as a communication medium. It can be used for long distances without the need for signal enhancement. The optical fibers also offer high bandwidth capacities with a single fiber, being able to achieve transfer rates of up to 40 Gigabit/second.

Optical fiber cables are simpler to tap than are generally believed. There are various optical fiber tapping methods. Splicing is the easiest form of tapping but it is detectable by most network security systems. Splicing will create a momentary lapse of data and is noticeable. More advanced tapping methods include injecting additional light into fiber cables and deducing the underlying optical signal by gauging certain interactions between the two. Bending fiber to create micro-bends can make light leak from the fiber without disrupting communication. This method is preferred in this context.

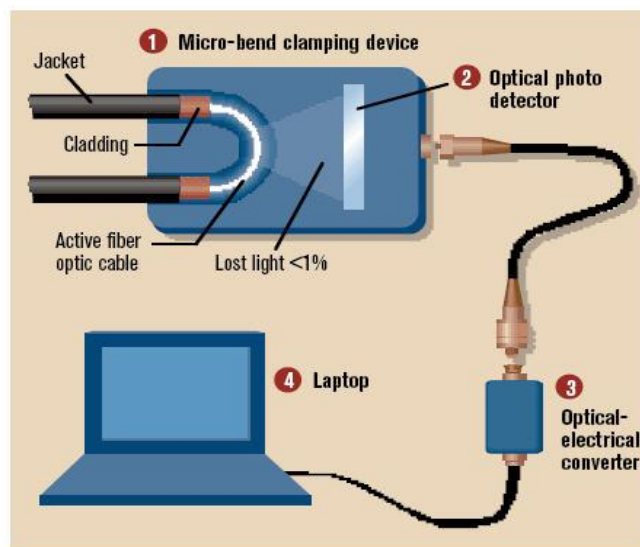


Fig. 3.6. An example of tapping

Source: <http://blogs.techrepublic.com.com/security/?p=222&tag=leftCol;post-223>.



Fig. 3.7. The actual tap hardware

Source: <http://blogs.techrepublic.com.com/security/?p=222&tag=leftCol;post-223>.

As described in reference [53], a hacker can purchase inexpensive hardware necessary to tap into a fiber. The tap consists of bending the fiber to a point that it leaks light, as shown in Fig. 3.6. A fiber cable is placed into a micro-bend clamping device. Then light leaks from the cable. An optical photo detector detects the leaking light and sends it to an optical-electrical converter. A converter changes the light pulses to electrical information and sends it to the hacker's PC through an Ethernet cable. Fig. 3.7 is a photograph of actual tap hardware.

Moreover, some tapping devices may be utilized not just for passive sniffing, but for active tapping, according to Oyster Optics [54]. Through such devices, a hacker is able to inject malicious signals into fiber cables. Those attacks are not detectable in real time. They are also difficult to locate, since the optical taps are subtle in nature.

Fiber taps present a high risk for SCADA systems of wind farms. Wind farms are built on open ground, and many of them are not staffed. Hackers can gain physical access

to fiber optics. Although the fiber cables are normally buried underground, they can dig holes in order to reach the cables.

Virtual Private Network (r₆)

Virtual Private Network (VPN) over the Internet is used in wind farm SCADA systems for remote communication. The IP Security (IPSEC) suite of protocols is commonly used to implement VPN. It offers authentication and encryption at the Internet Protocol (IP) packet level.

DoS attacks using a Botnet or other means (e.g., SYN Flooding) cause a large number of compromised computers to flood a huge volume of network traffic toward a target server or a subnet to the extent of affecting or destabilizing the victim. When such an attack happens in a VPN, the data transmission rate will be severely affected.

DoS attack may not disturb real-time operations of wind farms severely, as wind farm SCADA systems are highly-automated. However, hackers can use DoS attack to facilitate some other attacks. DoS attack can be used to block monitoring and control operations of wind farm operators so that other attacks are able to proceed.

Digital Microwave (r₇)

Licensed digital microwave changes the continuous signal used by analog microwave to a digital signal. This allows for greater data transmission rates with better data integrity. It is commonly used within control WANs.

Digital microwave radio point-to-point communications may be encrypted using a variety of technologies. Current vendor offerings include the use of OpenSSL protocol suite to the National Security Agency (NSA) Type 1. Encryption does impact the data transfer rate associated with the link.

Poor access control within a control room (r₈)

The idea of access control is to grant no more than necessary access to each user. An appropriate access control policy is extremely critical to cyber security. However, perfect access control is almost impossible to achieve due to the scale and complexity of cyber systems. Poor access control will grant some users inappropriate levels of access, leading to security vulnerabilities.

Poor access control within a control center (r₉)

Same as above.

Bad configuration of remote access (r₁₀)

Remote access is exposed to public. If not secured properly, it will be the start point of cyber attacks.

Weak firewall policy (r₁₁)

Weak firewall policy results in unwanted inbound and outbound traffic.

Human errors (r₁₂)

Human errors can interfere with normal operations of SCADA systems. A trusted user of SCADA systems can cause an internal attack. Hackers outside may gain access to SCADA systems through malware introduced by phishing and infected portable storage devices. Oversight or negligence during key generation, distribution and management could cause critical information to be corrupted.

3.4.3 DERFEM and Attack Graph

The vulnerabilities are evaluated through DERFEM. The results are shown in Table 3.2. An attack graph is built as shown in Fig. 3.8. Nine possible intrusion scenarios are identified; the probability of occurrence of every scenario is calculated, shown in

Table 3.3.

Table 3.2. The results of DERFEM

	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8	r_9	r_{10}	r_{11}	r_{12}	$Vul(r_i)$
r_1	1	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	1
r_2	0.6	1	0.9	0.7	0.5	0.8	0.8	0.6	0.6	0.5	0.6	0.4	0.75
r_3	0.4	0.6	1	0.5	0.4	0.7	0.8	0.3	0.2	0.3	0.2	0.5	0.5
r_4	0.5	0.4	0.6	1	0.7	0.7	0.7	0.6	0.5	0.4	0.6	0.5	0.5714
r_5	0.4	0.3	0.3	0.4	1	0.3	0.3	0.5	0.5	0.6	0.5	0.6	0.5
r_6	0.2	0.2	0.3	0.2	0.2	1	0.3	0.2	0.2	0.3	0.2	0.2	0.25
r_7	0.1	0.1	0.2	0.1	0.1	0.1	1	0.1	0.1	0.2	0.1	0.1	0.125
r_8	0.5	0.5	0.5	0.5	0.4	0.6	0.3	1	0.4	0.5	0.4	0.4	0.625
r_9	0.2	0.3	0.1	0.3	0.2	0.2	0.2	0.2	1	0.2	0.2	0.1	0.25
r_{10}	0.7	0.4	0.6	0.5	0.4	0.6	0.5	0.6	0.6	1	0.6	0.4	0.6667
r_{11}	0.4	0.5	0.4	0.5	0.4	0.5	0.3	0.5	0.5	0.5	1	0.5	0.5
r_{12}	0.3	0.3	0.4	0.3	0.3	0.2	0.2	0.3	0.3	0.3	0.2	1	0.375

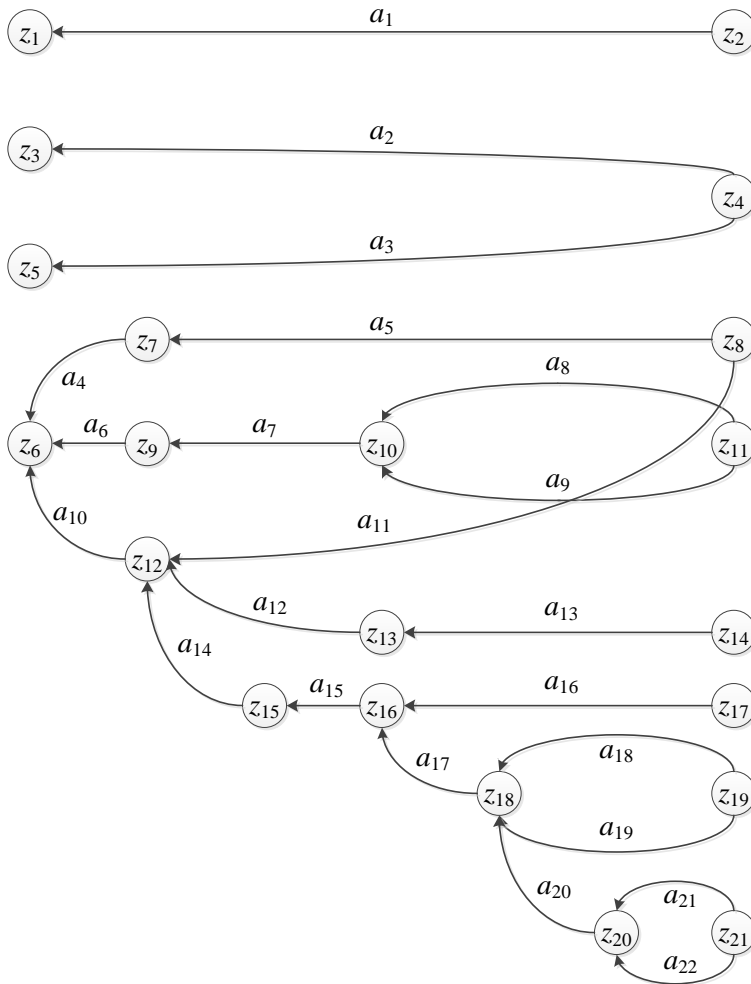


Fig. 3.8. The constructed attack graph

- z_1 (Hacker, WTCP, 5)
- z_2 (Hacker, WTCP, 0)
- z_3 (Hacker, WTCPs in a wind farm, 2)
- z_4 (Hacker, WTCPs in a wind farm, 0)
- z_5 (Hacker, WTCPs in a wind farm, 1)
- z_6 (Hacker, WTCPs in a wind farm, 4)
- z_7 (Hacker, SCADA server in the control room, 3)
- z_8 (Hacker, SCADA server in the control room, 0)
- z_9 (Hacker, SCADA server in the control room, 4)
- z_{10} (Hacker, SCADA server in the control center, 2)
- z_{11} (Hacker, SCADA server in the control center, 0)
- z_{12} (Hacker, SCADA server in the control room, 5)
- z_{13} (Hacker, workstation in the control room, 5)
- z_{14} (Hacker, workstation in the control room, 0)
- z_{15} (Hacker, SCADA server in the control center, 5)
- z_{16} (Hacker, workstation in the control center, 5)
- z_{17} (Hacker, workstation in the control center, 0)
- z_{18} (Hacker, workstation in the corporate LAN, 5)
- z_{19} (Hacker, workstation in the corporate LAN, 0)
- z_{20} (Hacker, remote access point, 5)
- z_{21} (Hacker, remote access point, 0)
- a_1 (Password cracking, z_2, z_1, r_1)
- a_2 (Jamming, z_4, z_3, r_4)

- a_3 (Passive tapping, z_4, z_5, r_5)
- a_4 (Man-in-the-middle attack, z_7, z_6, r_2)
- a_5 (Active tapping, z_8, z_7, r_5)
- a_6 (Spoof, z_9, z_6, r_2)
- a_7 (Spoof, z_{10}, z_9, r_3)
- a_8 (DOS attack, z_{11}, z_{10}, r_6)
- a_9 (Jamming, z_{11}, z_{10}, r_7)
- a_{10} (Spoof, z_{12}, z_6, r_2)
- a_{11} (Internal attack, z_8, z_{12}, r_{12})
- a_{12} (Malware infection, z_{13}, z_{12}, r_8)
- a_{13} (Infected portable storage device attack, z_{14}, z_{13}, r_{12})
- a_{14} (Malware infection, z_{15}, z_{12}, r_3)
- a_{15} (Malware infection, z_{16}, z_{15}, r_9)
- a_{16} (Infected portable storage device attack, z_{17}, z_{16}, r_{12})
- a_{17} (Malware infection, z_{18}, z_{16}, r_{11})
- a_{18} (Infected portable storage device attack, z_{19}, z_{18}, r_{12})
- a_{19} (Phishing, z_{19}, z_{18}, r_{12})
- a_{20} (Malware infection, z_{20}, z_{18}, r_{10})
- a_{21} (Infected portable storage device attack, z_{21}, z_{20}, r_{12})
- a_{22} (Phishing, z_{21}, z_{20}, r_{12})

The intrusion scenarios show that, if successfully executed, a hacker will gain some levels of control access to several or even hundreds of WTCs. The power output of compromised wind farms will be maliciously manipulated. The impact on power

system dynamics is studied next.

Table 3.3. The intrusion scenarios and the probabilities

Intrusion scenario	Probability
a_1	1
a_2	0.5714
a_3	0.5
$a_5 \rightarrow a_4$ OR $a_{11} \rightarrow a_{10}$	0.5508
a_8 (OR a_9) $\rightarrow a_7 \rightarrow a_6$	0.1289
$a_{13} \rightarrow a_{12} \rightarrow a_{10}$	0.1758
$a_{16} \rightarrow a_{15} \rightarrow a_{14} \rightarrow a_{10}$	0.0352
a_{18} (OR a_{19}) $\rightarrow a_{17} \rightarrow a_{15} \rightarrow a_{14} \rightarrow a_{10}$	0.0176
a_{21} (OR a_{22}) $\rightarrow a_{20} \rightarrow a_{17} \rightarrow a_{15} \rightarrow a_{14} \rightarrow a_{10}$	0.0117

3.4.4 Simulation Results

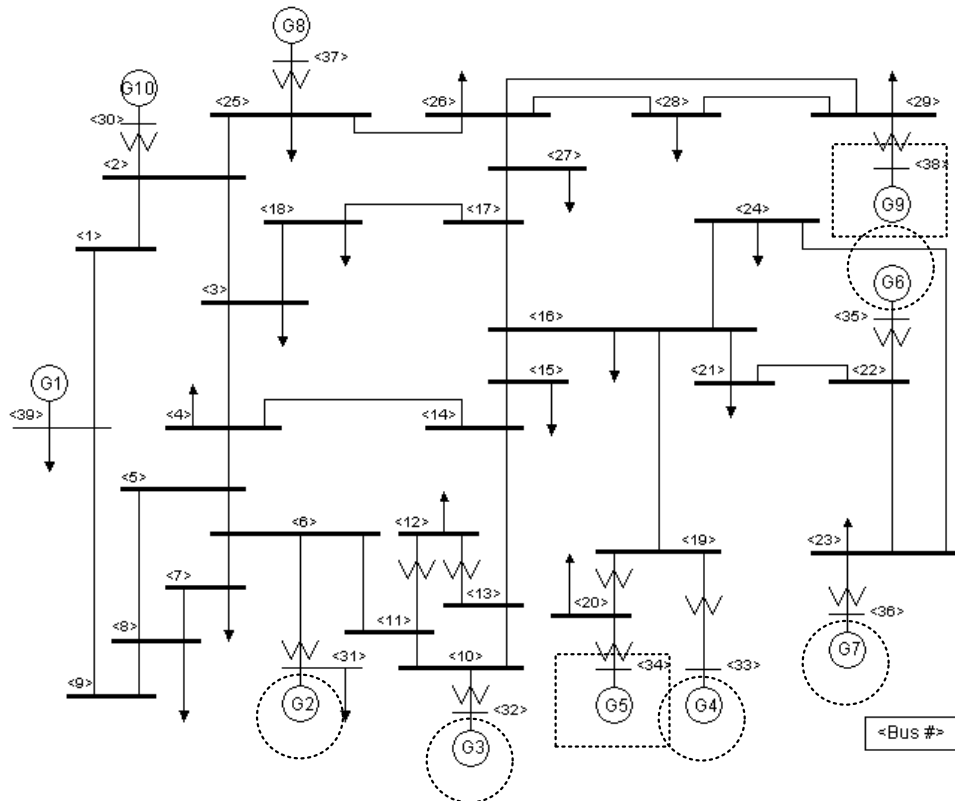


Fig. 3.9. IEEE 10 Generator 39 Bus System

The IEEE 39 bus system [55] is used for simulations, shown in Fig. 3.9.

Generator G5 and G9 (marked with two rectangles) are replaced by two wind farms comprised of the variable speed wind turbines utilizing Doubly Fed Induction Generators (DFIGs). The rating value of a wind turbine is 2.0 MW. From the system's point of view, the wind farms are considered as constant negative loads during the transient period, due to the fast control capacity of the power electronic technology within wind turbines. The other generators are classically modeled; the loads are represented by ZIP models.

MCLEs are calculated for the generator buses (except G5 and G9) by the proposed algorithm every 0.2s to monitor power system stability. Suppose that at $t=0.4s$, a hacker maliciously manipulates the power output of G5 (or G9) to some extent. Part of the simulation results is shown in Table 3.4. The simulation results show that

- The values of MCLEs are close to 0, when the power system is in the steady state.
- Upon an attack, the values of MCLEs oscillate as time evolves, but have limited values if voltage instability is not likely to happen. During Attack 2, the reactive power output of G5 is reduced by 10 Mvar at $t=0.4s$. MCLEs increase for a while, and then decrease, as shown in Fig. 3.10(a). The values are below 200.
- The values of MCLEs constantly increase as time evolves, if voltage instability is likely to happen within the power system. During Attack 10, the reactive power output of G5 is reduced by half at $t=0.4s$. Voltage instability happens at $t=1.42s$, as shown in Fig. 3.10(c) and (d). The values of MCLEs keep increasing after the attack, as shown in Fig. 3.10(b).
- Voltage instability is likely to occur around the generator buses where

MCLEs have high values. Take Attack 10 as an example, MCLEs of G2, G3, G4, G6 and G7 (circled in Fig. 3.9) are over 1000 at $t=1.4s$. Time-domain simulation results show that voltage instability happens around those generator buses. It is reasonable as G2, G3, G4, G6 and G7 are close to G5.

Table 3.4. MCLE of bus G3

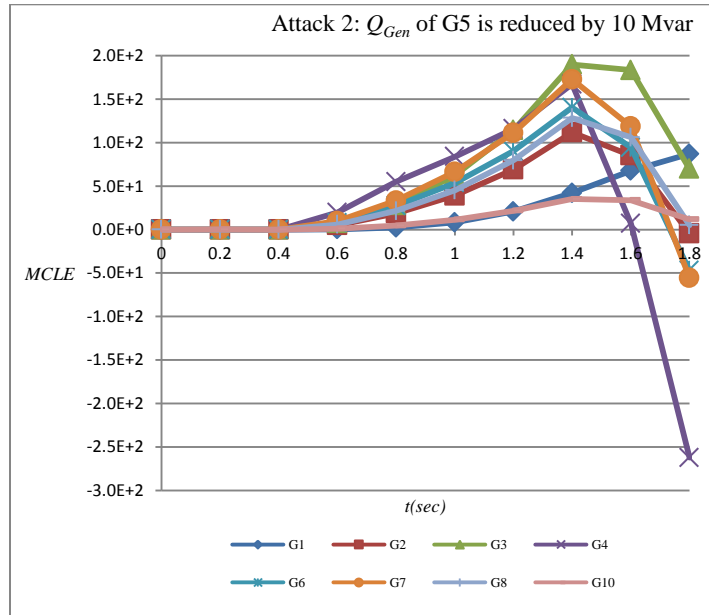
$MCLE_{G3}$	0-0.2s	0.2s-0.4s	0.4s-0.6s	0.6s-0.8s	0.8s-1s	1s-1.2s	1.2s-1.4s	1.4s-1.6s	1.6s-1.8s	Voltage Instability
Attack 1	-2.77E-3	-2.62E-2	9.88E-1	2.77	3.84	3.69	2.96	3.55	7.29	N/A
Attack 2	-2.77E-3	-2.62E-2	7.25	2.81E1	6.23E1	1.14E2	1.90E2	1.83E2	6.98E1	N/A
Attack 3	-2.77E-3	-2.62E-2	6.90E1	2.11E2	3.94E2	6.83E2	1.22E3			$t=1.57s$
Attack 4	-2.77E-3	-2.62E-2	1.17E2	4.08E2	9.12E2	1.98E3				$t=1.20s$
Attack 5	-2.77E-3	-2.62E-2	-1.01	-2.27	-3.16	-4.08	-4.58	-4.23	-2.78	N/A
Attack 6	-2.77E-3	-2.62E-2	6.04	2.21E1	4.65E1	8.18E1	1.32E2	1.09E2	4.81	N/A
Attack 7	-2.77E-3	-2.62E-2	3.45E1	1.05E2	2.00E2	3.51E2	6.12E2	1.10E3	2.17E3	$t=1.86s$
Attack 8	-2.77E-3	-2.62E-2	1.05E2	3.48E2	7.27E2	1.43E3				$t=1.24s$
Attack 9	-2.77E-3	-2.62E-2	2.31E2	7.65E2	1.72E3					$t=1.03s$
Attack 10	-2.77E-3	-2.62E-2	7.12E1	2.45E2	5.27E2	1.03E3	2.05E3			$t=1.42s$
Attack 11	-2.77E-3	-2.62E-2	3.55E2	1.37E3						$t=0.8s$
Attack 12	-2.77E-3	-2.62E-2	2.91E2	1.03E3	2.72E3					$t=1.06s$
Attack 13	-2.77E-3	-2.62E-2	8.33E2							$t=0.76s$
Attack 14	-2.77E-3	-2.62E-2	6.43E1	2.07E2	4.10E2	7.47E2	1.38E3			$t=1.56s$

- Attack 1 P_{Gen} of G5 is reduced by 10 MW
- Attack 2 Q_{Gen} of G5 is reduced by 10 Mvar
- Attack 3 P_{Gen} of G5 is reduced by 100 MW
- Attack 4 Q_{Gen} of G5 is reduced by 100 Mvar
- Attack 5 P_{Gen} of G9 is reduced by 10 MW
- Attack 6 Q_{Gen} of G9 is reduced by 7.5 Mvar
- Attack 7 P_{Gen} of G9 is reduced by 100 MW
- Attack 8 Q_{Gen} of G9 is reduced by 75 Mvar
- Attack 9 P_{Gen} of G5 is reduced by half
- Attack 10 Q_{Gen} of G5 is reduced by half
- Attack 11 Q_{Gen} of G5 is reduced to $-Q_{Gen}$

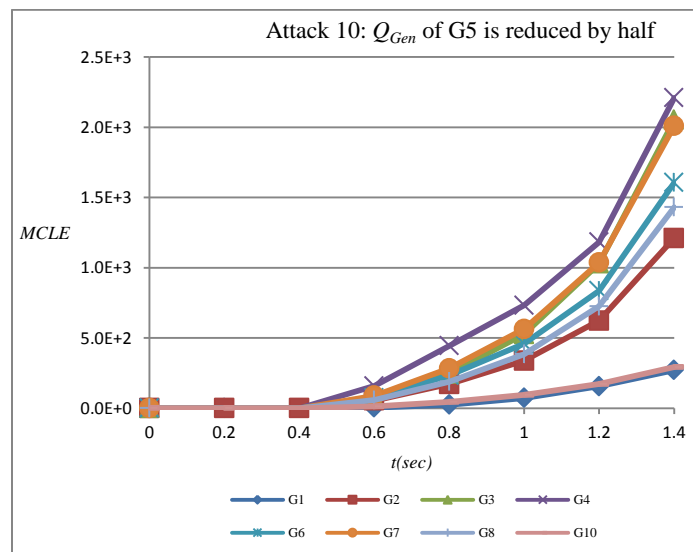
Attack 12 P_{Gen} of G9 is reduced by half

Attack 13 P_{Gen} of G5 is reduced by half; Q_{Gen} of G5 is reduced by half; P_{Gen} of G9 is reduced by half

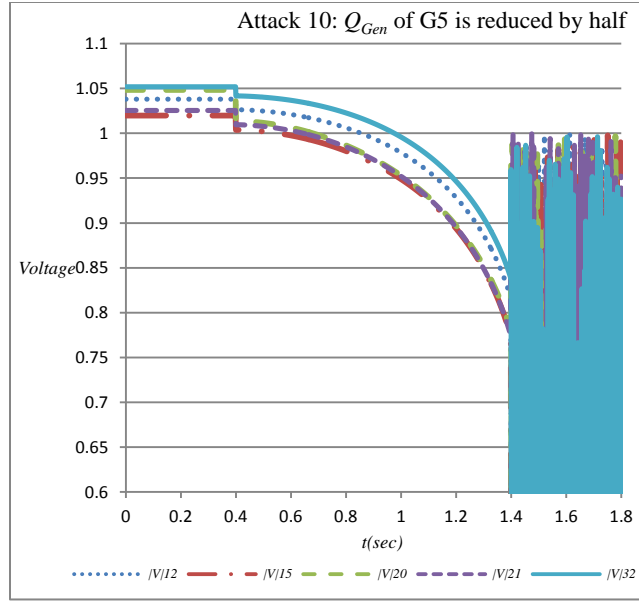
Attack 14 P_{Gen} of G5 is reduced by 30 MW; Q_{Gen} of G5 is reduced by 15 Mvar; P_{Gen} of G9 is reduced by 50 MW; Q_{Gen} of G9 is reduced by 10 Mvar



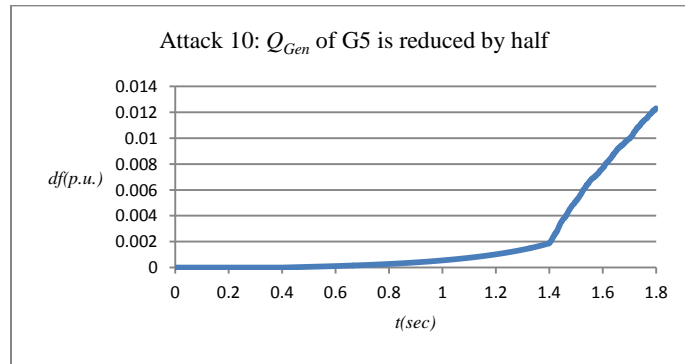
(a)



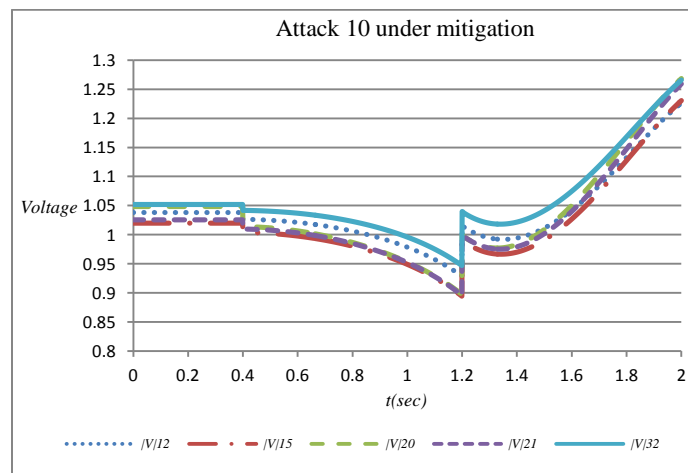
(b)



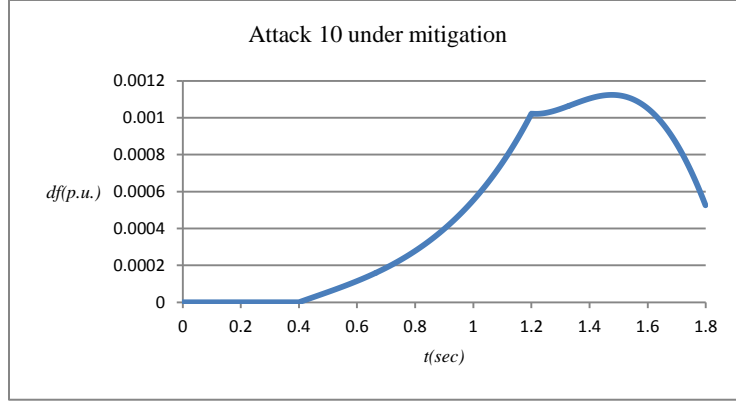
(c)



(d)



(e)



(f)

Fig. 3.10. The simulation results

Based on the simulation results, a predefined limit for values of MCLEs is set to be 800. If the value of MCLE of a generator bus exceeds the limit, it is predicted that voltage instability will happen around the generator bus. Control signal

$$E_{Gen}^{ref,new} = (1 + MCLE/10000)E_{Gen}^{ref,old}$$

will be sent to the excitation system of the related generator. Simulation results show that voltage instability can be avoided. For example, during Attack 10, MCLEs of G3, G4, G6 and G7 are over 800 at $t=1.2s$. The corresponding control signals are then sent to G3, G4, G6 and G7. Voltage instability is prevented, as shown in Fig. 3.10(e) and (f).

3.5 Discussion

A risk assessment framework with a PMU-based IRS is proposed for power control systems. The main idea of IRS is to calculate MCLEs for generator buses, in order to monitor voltage stability. The higher values MCLEs have, the more likely voltage instability can occur around the corresponding generator buses. MCLE method is based on a solid analytical foundation and it is validated by simulation results.

CHAPTER 4. CONCLUSIONS

This research leads to significant contributions to the development of a more reliable and secure power grid. A new method is proposed to prevent power systems from a loss of synchronism; a risk assessment framework is developed to mitigate the impact of cyber attacks on power system dynamics. The Lyapunov Exponents are applied to the analysis of power system dynamics. This work also results in an innovative application of PMU data. As large scale deployment of PMUs on power grids continues, it is important to develop new applications of PMU data. It is believed that this research is an important step toward the goal.

Future research includes:

- 1) For a large power system with numerous generators, it is difficult to establish a dynamical system model to represent the power system during a contingency. The power system model may be simplified based on reasonable assumptions. For example, multiple generators that tend to swing together may be represented by an aggregated model.
- 2) As power systems grow in scale and complexity, it may be more difficult to determine the time interval length for MLE merely by the proposed spectrum analysis. An on-line pattern recognition technique coupled with spectrum analysis may be used to determine the size of T . The dynamic patterns in a power system can be divided into classes, e.g., fast and slow. Each pattern of dynamic variations is to be assigned a different time interval length T based on spectrum analysis of the power swings following disturbances. When a disturbance occurs, a pattern recognition

technique is used to recognize the type of perturbation. A fast perturbation can be detected by a short time window, while a slow pattern will require a longer time window. MLE is then calculated over the corresponding time interval length T .

- 3) Further work is needed to draw a definitive conclusion about the relationship between the value of MLE and the size of stability margin.
- 4) For a large cyber system with numerous security vulnerabilities, DERFEM may not be sufficient. Some statistical analysis techniques may be coupled with DERFEM to improve evaluation results.
- 5) A dedicated control strategy can be developed in IRS for the control actions to prevent voltage instability. It will require advanced knowledge of generator excitation systems.
- 6) Many new PMUs will be installed in the future. The placement of new PMUs for complete observability should be investigated. An integer quadratic programming approach [56] may be used for an optimal placement of PMUs. Complete observability should be ensured under normal as well as contingency operating conditions.

PUBLICATIONS

- Journals

J. Yan, C. C. Liu, and U. Vaidya, "PMU-based monitoring of rotor angle dynamics," Accepted for publication in *IEEE Trans. Power Syst.*

J. Yan, M. Govindarasu, C. C. Liu, and U. Vaidya, "Risk assessment for cyber security of the Power Grid," To be submitted to *IEEE Trans. Power Syst.*

- Conferences

J. Yan, C. C. Liu, and M. Govindarasu, "Cyber intrusion of wind farm SCADA system and its impact analysis," *IEEE PES. Power Systems Conference and Exposition*, Phoenix, Arizona, March 2011.

BIBLIOGRAPHY

- [1] WSCC, "Western Systems Coordinating Council (WSCC) disturbance report for the power system outage that occurred on the western interconnection, August 10, 1996," approved by the WSCC Operations Committee on October 18, 1996.
- [2] U.S.-Canada Power System Outage Task Force, "Final report on the August 14th blackout in the United States and Canada," United States Department of Energy and National Resources Canada, April 2004. [Online] available: <https://reports.energy.gov/BlackoutFinal-Web.pdf>
- [3] UCTE, "Final report of the investigation committee on the 28 September 2003 blackout in Italy," April 2004. [Online] available: http://www.ucte.org/library/otherreports/20040427_UCTE_IC_Final_report.pdf
- [4] UCTE, "Final report on the disturbances of 4 November 2006," January 2007. [Online] available: <http://www.ucte.org/library/otherreports/Final-Report-20070130.pdf>
- [5] B. Parks, "Transforming the grid to revolutionize electric power in North America," U.S. Department of Energy, Edison Electric Institute: Fall 2003 Transmission, Distribution and Metering Conference, October 13, 2003.
- [6] K. Yamashita, J. Li, P. Zhang, and C. C. Liu, "Analysis and control of major blackout events," *IEEE PES. Power Systems Conference and Exposition*, pp. 1-4, Seattle, WA, March 2009.
- [7] C. C. Liu, J. Jung, G. T. Heydt, V. Vittal, and A. Phadke, "The strategic power infrastructure defense (SPID) system," *IEEE Control System Magazine*, pp. 40-52, August 2000.

- [8] C. Gonzalez-Perez, and B. F. Wollenberg, "Analysis of massive measurement loss in large-scale power system state estimation," *IEEE Trans. Power Syst.*, vol. 16, no. 4, pp. 825-832, November 2001.
- [9] R. Lambert, E. Tarasiewicz, A. Xemard, and G. Fleury, "Probabilistic evaluation of lightning-related failure of power system apparatus," *IEEE Trans. Power Delivery*, vol. 18, no. 2, pp. 579-586, April 2003.
- [10] M. Chow and L. S. Taylor, "Analysis and prevention of animal-caused faults in power distribution systems," *IEEE Trans. Power Delivery*, vol. 10, no. 2, pp. 995-1001, April 1995.
- [11] D. Q. Zhou, U. D. Annakkage, and A. D. Rajapakse, "Online monitoring of voltage stability margin using an artificial neural network," *IEEE Trans. Power Syst.*, vol. 25, no. 3, pp. 1566-1574, August 2010.
- [12] T. Amraee, A. M. Ranjbar, R. Feuillet, and B. Mozafari, "System protection scheme for mitigation of cascaded voltage collapses," *IET Generation, Transmission & Distribution*, vol. 3, no. 3, pp. 242-256, March 2009.
- [13] A. G. Bahbah and A. A. Girgis, "New method for generators' angles and angular velocities prediction for transient stability assessment of multimachine power systems using recurrent artificial neural network," *IEEE Trans. Power Syst.*, vol. 19, no. 2, pp. 1015-1022, May 2004.
- [14] M. Larsson and C. Rehtanz, "Predictive frequency stability control based on wide-area phasor measurements," *Proc. IEEE Power Engineering Society Summer Meeting*, vol. 1, pp. 233-238, Chicago, IL, July 2002.

- [15] J. Li, C. C. Liu, and K. Schneider, "Controlled partitioning of a power network considering real and reactive power balance," *IEEE Trans. Smart Grid*, vol. 1, no. 3, pp. 261-269, December 2010.
- [16] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- [17] V. Centeno, A. G. Phadke, A. Edris, J. Benton, M. Gaudi, and G. Michel, "An adaptive out-of-step relay for power system protection," *IEEE Trans. Power Delivery*, vol. 12, no. 1, pp. 61-71, January 1997.
- [18] V. Centeno, A. G. Phadke, and A. Edris, "Adaptive out-of-step relay with phasor measurement," *Developments in Power System Protection, Sixth International Conference*, Conf. pub 1, no. 434, pp. 210-213, March 1997.
- [19] V. Centeno, A. G. Phadke, A. Edris, J. Benton, and G. Michel, "An adaptive out-of-step relay," *IEEE Power Engineering Review*, vol. 17, no. 1, pp. 39-40, January 1997.
- [20] V. Centeno, J. de la Ree, A. G. Phadke, G. Michel, R. J. Murphy, and R. O. Burnett, Jr., "Adaptive out-of-step relaying using phasor measurement techniques," *IEEE Computer Application in Power*, vol. 6, no. 4, pp. 12-17, October 1993.
- [21] J. H. Chow, A. Chakraborty, M. Arca, B. Bhargava, and A. Salazar, "Synchronized phasor data based energy function analysis of dominant power transfer paths in large power systems," *IEEE Trans. Power Syst.*, vol. 22, no. 2, pp. 727-734, May 2007.

- [22] K. Yamashita and H. Kameda, "Out-of-step prediction logic for wide-area protection based on an autoregressive model," *IEEE PES. Power Systems Conference and Exposition*, vol. 1, pp. 307-312, October 2004.
- [23] N. Kakimoto, M. Sugumi, T. Makino, and K. Tomiyama, "Monitoring of interarea oscillation mode by synchronized phasor measurement," *IEEE Trans. Power Syst.*, vol. 21, no. 1, pp. 260-268, February 2006.
- [24] C. W. Liu and J. Thorp, "New methods for computing power system dynamic response for real-time transient stability prediction," *IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, no. 3, pp. 324-337, March 2000.
- [25] C. Liu, M. Su, S. Tsay, and Y. Wang, "Application of a novel fuzzy neural network to real-time transient stability swings prediction based on synchronized phasor measurements," *IEEE Trans. Power Syst.*, vol. 14, no. 2, pp. 685-692, May 1999.
- [26] K. Sun, S. Likhate, V. Vittal, V. S. Kolluri, and S. Mandal, "An online dynamic security assessment scheme using phasor measurements and decision trees," *IEEE Trans. Power Syst.*, vol. 22, no. 4, pp. 1935-1943, November 2007.
- [27] I. Kamwa, S. R. Samantaray, and G. Joos, "Development of rule-based classifiers for rapid stability assessment of wide-area post-disturbance records," *IEEE Trans. Power Syst.*, vol. 24, no. 1, pp. 258-270, February 2009.
- [28] A. Del Angel, P. Geurts, D. Ernst, M. Glavic, and L. Wehenkel, "Estimation of rotor angles of synchronous machines using artificial neural networks and local

- PMU-based quantities,” *Neurocomputing, Elsevier*, vol. 70, no. 16-18, pp. 2668-2678, October 2007.
- [29] C. Liu, J. S. Thorp, J. Lu, R. J. Thomas, and H. Chiang, “Detection of transiently chaotic swings in power systems using real-time phasor measurements,” *IEEE Trans. Power Syst.*, vol. 9, no. 3, pp. 1285-1292, August 1994.
- [30] V. I. Oseledec, “Multiplicative ergodic theorem: Lyapunov characteristic exponent for dynamical systems,” *Moscow Math. Soc.*, vol. 19, pp. 539-575, 1968.
- [31] J. P. Eckman and D. Ruelle, “Ergodic theory of chaos and strange attractors,” *Rev. Modern Phys.*, vol. 57, pp. 617-656, 1985.
- [32] H. K. Khalil, *Nonlinear Systems (Third Edition)*. Upper Saddle River, NJ: Prentice Hall, 2002.
- [33] K. Ramasubramanian and M. S. Sriram, “A comparative study of computation of Lyapunov spectra with different algorithms,” *Physica D*, vol. 139, issue 1-2, pp. 72-86, May 2000.
- [34] K. Yamashita, S. K. Joo, J. Li, P. Zhang, and C. C. Liu, “Analysis, control and economic impact assessment of major blackout events,” *European Trans. Electrical Power*, vol. 18, no. 8, pp. 854-871, November 2008.
- [35] http://www.oe.energy.gov/DocumentsandMedia/Roadmap_to_Secure_Control_Systems_in_the_Energy_Sector.pdf
- [36] <http://www.nerc.com/page.php?cid=2|20>

- [37] F. Cleveland, "IEC TC57 security standards for power system's information infrastructure—Beyond simple encryption," *Proc. IEEE Power Eng. Soc. General Meeting*, Tampa, FL, 2007.
- [38] F. Sheldon, S. Batsell, S. Prowell, and M. Langston, Control Systems Cybersecurity Awareness. Washington DC: U.S. Comput. Emergency Readiness Team (CERT), pp. 1-10, July 25, 2005.
- [39] J. Depoy, J. Phelan, P. Sholander, B. Smith, G. Varnado, and G. Wyss, "Risk assessment for physical and cyber-attacks on critical infrastructures," *Proc. IEEE MILCOM*, vol. 3, pp. 1961-1969, October 17-20, 2005.
- [40] C. W. Ten, G. Maninaran, and C. C. Liu, "Cybersecurity for critical infrastructures: attack and defense modeling," *IEEE Trans. Power Syst.*, vol. 40, no. 4, pp. 853-865, July 2010.
- [41] C. W. Ten, C. C. Liu, and G. Maninaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836-1846, November 2008.
- [42] O. M. Sheyner, "Scenario graphs and attack graphs," *Ph.D. dissertation*, Dept. Comput. Sci., Carnegie Mellon Univ., Pittsburgh, PA, 2004.
- [43] L. M. Pecora, T. L. Carroll, *Phys. Rev. Lett.* 64 (1990) 82 I.
- [44] L. M. Pecora, T. L. Carroll, *Phys. Rev. A* 44 (1991) 2374.
- [45] R. Vilela Mendes, "Conditional exponents, entropies and a measure of dynamical self-organization," *Physics Letters A*, 248 (1998) 167-171.
- [46] American Wind Energy Association: 2009. Another Record Year for Wind Energy Installations.

- [47] U.S. Department of Energy: 2008. 20% Wind Energy by 2030. DOE/GO-102008-2567. Washington, DC.
- [48] A. D. Hansen, C. Jauch, P. Sørensen, F. Iov, and F. Blaabjerg, “Dynamic wind turbine models in power system simulation tool DIgSILENT,” Risø-R-1400(EN), Risø National Laboratory, 2004.
- [49] P. Sørensen, B. Bak-Jensen, J. Kristiansen, A. D. Hansen, L. Janosi, and J. Bech, “Power plant characteristics of wind farms, wind power for the 21st century,” *Proc. International Conference*, Kassel, Germany, September 2000.
- [50] B. Badrzadeh, M. Bradt, N. Castillo, R. Janakiraman, R. Kennedy, S. Klein, T. Smith, and L. Vargas (IEEE PES Wind Plant Collector System Design Working Group), “Wind power plant SCADA and controls,” *IEEE PES General Meeting*, pp. 1-7, July 2011.
- [51] E. Brier, D. Naccache, and P. Paillier, “Chemical combinatorial attacks on keyboards,” *International Association for Cryptographic Research ePrint Archive 2003*, 217 (2003).
- [52] <http://www.arcadiannetworks.com/article.aspx?MID=5000&CID=8071>
- [53] <http://blogs.techrepublic.com.com/security/?p=222&tag=leftCol;post-223>.
- [54] Oyster Optics, Inc., “Securing fiber optic communications against optical tapping methods,” [Online] available: http://www.rootsecure.net/content/downloads/pdf/fiber_optic_taps.pdf
- [55] sys.elec.kitami-it.ac.jp/ueda/demo/WebPF/39-New-England.pdf

- [56] S. Chakrabarti, E. Kyriakides, and D. Eliades, "Placement of synchronized measurements for power system observability", *IEEE Trans. Power Delivery*, vol. 24, no. 1, pp. 12-19, January 2009.

ACKNOWLEDGEMENTS

This dissertation is a material proof that education CAN and WILL provide a brighter future for every person in the world; all it takes is a dream and an opportunity.

I have no word to express all my gratitude and appreciation to my advisor Dr. Chen-Ching Liu. His patience, generosity, guidance, friendship and immense knowledge have been critical in my Ph.D. study and I would be lost without his help. I also gratefully appreciate the financial support that he has given to me for all these years.

A special thanks to Dr. Manimaran Govindarasu, Dr. Umesh Vaidya, Dr. Venkataramana Ajjarapu, and Dr. Lizhi, Wang for everything that I learned from them, inside and outside the classroom. All the skills gained from your courses and talks will certainly guide me in making decisions throughout my professional life.

I would also like to thank my fellow graduate students and the ECpE staff, with whom I have had valorous and helpful discussions regarding everything one can possibly imagine.

The financial support from the National Science Foundation (Grant CNS 0915945) and Electric Power Research Center, ISU, is greatly appreciated.